



CITY COUNCIL MEETING & PUBLIC HEARING SEPTEMBER 26, 2022

ALPHARETTA CITY HALL
COUNCIL CHAMBERS
2 PARK PLAZA
6:30 PM

I. CALL TO ORDER

II. ROLL CALL

III. PLEDGE TO THE FLAG

IV. CONSENT AGENDA

A. Council Meeting Minutes (Meeting of 9/19/2022)

Approval of the City Council Meeting Minutes from the meeting of September 19, 2022

B. Financial Management Report: Month Ending July 31, 2022

Approval of the Financial Management Report for the month ending July 31, 2022

C. Memorandum of Understanding: GDOT GA 400 Managed Lanes Utility

Approval of Public Private Partnership (P3) Memorandum of Understanding between the Georgia Department of Transportation and the City of Alpharetta to construct Express Lanes along Georgia State Route 400

D. Palo Alto Hardware Refresh

Approve the purchase and installation of replacement Palo Alto network security technology to Layer3 Communications, LLC

E. Managed Print Services, RFP 22-124

Approval of the award of RFP 22-124 to EDGE Business Systems for managed print services

F. Fran Shoenthal McQueen Settlement Agreement

Approval of the Settlement Agreement and Full and Final Release of Claims by Fran Shoenthal McQueen and authorize the Mayor to execute all necessary documents.

G. Playground Equipment Replacement: Webb Bridge Park (Webb Zone)

REMOVED: This item has been removed from the Consent Agenda by City Staff and will not be heard, discussed, or considered during tonight's meeting.

V. PUBLIC HEARING

A. Z-22-13 / V-22-25 / Grand Communities / 2325 Old Milton Parkway

Consideration of a rezoning and variances to allow for the construction of 24 'For-Sale townhomes on approximately 6.15 acres. A rezoning is requested from O-I (Office-Institutional) and R-12 (Dwelling, 'For-Sale', Residential) to DT-LW (Downtown Live-Work) and variances are requested to reduce stream buffers, allow some townhomes to be front loaded, modify streetscape standards, and reduce undisturbed buffers. The property is located at 2325 Old Milton Parkway, 0 Norcross Street, and 210 Norcross Street and is legally described as being located in Land Lot 748, 1st District, 2nd Section, Fulton County, Georgia.

B. PH-21-06 Kairos/Thompson Street Flats Change to Condition of Zoning

WITHDRAWN: This item has been withdrawn by the applicant and will not be considered at the September 26, 2022 City Council meeting.

Consideration of a request to change previous conditions of zoning to allow for a change from 12 'For-Sale' condominium units to 10 'For-Sale' single-family detached homes. The property is located at 51 and 61 Thompson Street and is legally described as being located in Land Lot 748, 1st District, 2nd Section, Fulton County, Georgia.

VI. OLD BUSINESS

A. PH-22-10 / Unified Development Code (UDC) Text Amendment - Banner Signs

Second Reading

Public Hearing #1 and First Reading occurred during the September 19, 2022 City Council Meeting & Public Hearing.

Consideration of text amendments to the Unified Development Code related to banner signs and allowing the Director of Community Development to approve an extension to the period of time that a business may display a banner sign when the business has frontage on a road that is under construction.

VII. NEW BUSINESS

A. Design Services: Pedestrian Safety Improvements (RFQ 22-1007)

Approval of the award of RFQ 22-1007 (Pedestrian Safety Improvement Design Services) and Roswell Street Alpha Loop Design Services (Old Milton Parkway to Old Roswell Street) to Moffatt & Nichol.

B. Design/Project Management Services Change Orders for Webb Bridge Road (North Point Parkway to City Limits)

Approval of Change Order #3 to Purchase Order 19000583 for Pond & Company and Change Order #2 to Purchase Order 19000584 for Atkins.

C. MS-ISAC Security Software

Approval of the purchase of the CIS Albert MD Appliance Primary Sensor System from the Center for Internet Security, Inc.

D. Windward / Highway 9 Area Strategic Master Plan

Approval of authorizing funding in an amount totaling \$60,000 to participate in the Windward/Highway 9 Masterplan LCI update study in partnership with the North Fulton CID and the City of Milton.

VIII. WORKSHOP ITEMS

A. Economic Development Strategic Plan Kickoff Presentation

IX. PUBLIC COMMENT

X. REPORTS

XI. EXECUTIVE SESSION (IF NECESSARY)

XII. ADJOURNMENT



STAFF REPORT

Submitting Department: City Clerk

Submitted By: Lauren Shapiro

Sponsored By:

Meeting Date: September 26, 2022

I. AGENDA ITEM TITLE: COUNCIL MEETING MINUTES (MEETING OF 9/19/2022)

APPROVAL OF THE CITY COUNCIL MEETING MINUTES FROM THE MEETING OF SEPTEMBER 19, 2022

II. RECOMMENDATION:

Approve the Council meeting minutes from September 19, 2022 at 6:30 p.m. as part of the Consent Agenda.

III. BUDGET IMPLICATIONS:

BUDGETED ITEM: NO

FISCAL IMPACT: NO

INCLUDED IN CURRENT FY CPTL BUDGET: NO

INCLUDED IN CURRENT FY OPRT. BUDGET: NO

TOTAL PROJECT COST:

APPROPRIATIONS:

<u>ACCOUNT TITLE/NUMBER</u>	<u>DOLLAR AMOUNT</u>
-----------------------------	----------------------

EXTERNAL FUNDING SOURCES:

<u>ACCOUNT TITLE/NUMBER</u>	<u>DOLLAR AMOUNT</u>
-----------------------------	----------------------

IV. REPORT IN BRIEF:

City Clerk, Lauren Shapiro, attended, recorded, and prepared a synopsis of the pertinent information that occurred during the City Council meeting on September 19, 2022 at 6:30 p.m.

V. ALTERNATIVES:

VI. ATTACHMENTS:

CC Meeting Minutes 9.19.2022



City Council Meeting & Public Hearing

SEPTEMBER 19, 2022

UNOFFICIAL MINUTES

Office of the City Clerk

ALPHARETTA CITY HALL

COUNCIL CHAMBERS | 2 PARK PLAZA | 6:30 PM

This action summary is provided as a convenience and service to the public, media, and staff. It is not the intent to record proceedings verbatim. Any reproduction of this summary must include this notice. This is not an official record of the Alpharetta City Council Meeting proceedings. City Council Meetings are recorded and available for review at <https://www.youtube.com/user/alpharettagov>.

I. CALL TO ORDER

- Mayor Gilvin called the meeting to order at 6:30p.m.

II. ROLL CALL

• Council Members

- Mayor Jim Gilvin
- Mayor Pro Tem Dan Merkel
- Donald F. Mitchell
- Douglas J. DeRito
- Brian Will

• Absent

- Jason Binder
- John Hipes

• Staff

- Chris Lagerbloom, City Administrator
- Molly Esswein, City Attorney with Jarrard & Davis
- James Drinkard, Asst. City Administrator
- Lauren Shapiro, City Clerk
- John Robison, Director of Public Safety
- Kathi Cook, Director of Community and Economic Development
- Morgan Rodgers, Director of Recreation, Parks, and Cultural Services
- Pete Sewczwicz, Director of Public Works

- Tom Harris, Director of Finance
- Adam Montgomery, Information Security Manager
- Eric Graves, Senior Transportation Engineer / Planner

III. PLEDGE TO THE FLAG

IV. CONSENT AGENDA

A. Council Meeting Minutes (Meeting of 8/22/2022)

B. Special Called City Council Meeting Minutes (Meeting of 9/1/2022)

C. Alcoholic Beverage License Applications

1. PH-22-AB-23 Buffalo Key West Connection, LLC

d/b/a Creation Social House

11500 Webb Bridge Way #A7, Alpharetta, GA 30005

Restaurant

Consumption on Premises

Liquor, Beer, Wine, & Sunday Sales

Owner: Buffalo Key West Connection, LLC

Registered Agent: Joseph Rampino

2. PH-22-AB-24 Arnold Mill Ventures, LLC

12335 Arnold Mill Road, Alpharetta, GA 30004

Convenience Store

Retail Package Sales

Beer, Wine, & Sunday Sales

Owner: Arnold Mill Ventures, LLC

Registered Agent: Shaheen Bijani

3. PH-22-AB-25 Ramen Spot GA, LLC

d/b/a Ramen Spot

7300 North Point Parkway, Suite 102 Alpharetta, GA 30022

Restaurant

Consumption on Premises

Liquor, Beer, Wine, & Sunday Sales

Owner: Ramen Spot GA, LLC

Registered Agent: Ben Yi Zhang

4. PH-22-AB-26 Lazy Dog Colorado OPS, LLC

d/b/a Lazy Dog Restaurant & Bar

10800 Haynes Bridge Road, Alpharetta, GA 30022

Restaurant

Consumption on Premises

Liquor, Beer, Wine & Sunday Sales
Owner: Lazy Dog Colorado OPS, LLC
Registered Agent: Michael Sard

5. **PH-22-AB-27 Sid's Pizza and Grill, LLC**
11770 Haynes Bridge Road, Alpharetta, GA 30009

Restaurant
Consumption on Premises
Beer, Wine, & Sunday Sales
Owner: Sid's Pizza and Grill, LLC
Registered Agent: Sharon Kurnett

6. **PH-22-AB-28 Phillips Brothers Hospitality Group, Inc.**
d/b/a Mercantile Social
20 North Main Street, Alpharetta, GA 30009

Restaurant
Consumption on Premises
Liquor, Beer, Wine, & Sunday Sales
Owner: Phillips Brothers Hospitality Group, Inc.
Registered Agent: Mark Phillips

- D. **FY2023 Law Enforcement Training Program Grant**
- E. **Approval of the Permanent Easement and Maintenance Agreement between Berberian Properties, LLC and the City of Alpharetta, and authorize the Mayor to execute all necessary documents.**
- F. **Approval of Conflict Waiver between the City of Milton and the City of Alpharetta, Georgia for the purposes of preparing an Intergovernmental Agreement with respect to housing of inmates at the Alpharetta Jail.**
- G. **Right of Entry, Indemnification and Maintenance Agreement between Pappas Restaurants, Inc. and the City of Alpharetta.**
- H. **Lost Intergovernmental Agreement: Cost Sharing**
Approval of an Intergovernmental Agreement by and among City of Alpharetta, Georgia, City of Atlanta, Georgia, City of Chattahoochee Hills, Georgia, City of College Park, Georgia, City of East Point, Georgia, City of Fairburn, Georgia, City of Hapeville, Georgia, City of Johns Creek, Georgia, City of Milton, Georgia, City of Mountain Park, Georgia, City of Palmetto, Georgia, City of Roswell, Georgia, City of South Fulton, Georgia, and City of Sandy Springs, Georgia for sharing of certain costs related to Local Option Sales Tax Negotiation with Fulton County, Georgia.

❖ **Council Member Mitchell offered a motion to approve the Consent Agenda.**

- **Mayor Pro Tem Merkel seconded the motion.**
- **The motion was approved unanimously (5-0).**

V. PRESENTATIONS & PROCLAMATIONS

A. Constitution Week 2022

- Mayor Gilvin presented representatives of the Patriots of Liberty Chapter of the National Society Daughters of the American Revolution with a proclamation for 2022 Constitution Week.

VI. PUBLIC HEARING

A. MP-22-03 / Z-22-05 / CU-22-02 / V-22-07 / North Point Redevelopment

DEFERRED: This item has been deferred by the applicant and will not be presented, heard, or discussed during this meeting. This item has been placed on the November 7, 2022 City Council Meeting & Public Hearing agenda.

Consideration of a master plan amendment, rezoning, conditional use and variances to allow for the demolition of approximately 464,000 square feet of the existing mall including 2 anchor boxes and redevelopment with 315,700 square feet of new retail, restaurants and creative office, 120,000 square feet of office, 150-room hotel, 900 'For-Rent' units, 36 'For-Sale' townhomes, and approximately 19 acres of open space on 83.67 acres. A master plan amendment is requested to the North Point Mall Master Plan to modify development regulations. A rezoning is requested from PSC (Planned Shopping Center) to MU (Mixed Use) and a conditional use is requested to allow Dwelling, 'For-Rent', Dwelling, 'For-Sale' Attached, and to increase the allowable density. Variances are requested to increase building height and encroach into the Georgia 400 buffer for the MARTA BRT and multi-use trail. The property is located at 1000 North Point Parkway, 4500 North Point Place, 0 & 5000 North Point Drive, 2000 & 6000 North Point Circle, and 0 Rock Mill Road and is legally described as being located in Land Lots 688, 689, 700, 701, 702, 742 & 743, 1st District, 2nd Section, Fulton County, Georgia.

B. PH-22-10 / Unified Development Code (UDC) Text Amendment – Banner Signs

Public Hearing & First Reading

Consideration of text amendments to the Unified Development Code related to banner signs and allowing the Director of Community Development to approve an extension to the period of time that a business may display a banner sign when the business has frontage on a road that is under construction.

- Director of Community and Economic Development, Kathi Cook, came forward to present this item.
- This item was considered at the 9/1/2022 Planning Commission meeting. There were no public comments. After discussion, Planning Commission recommended approval subject to changing 'retail and restaurant business' to 'commercial business' and adding the 'County' as it relates to roadway construction activities (7-0).
- Construction can have impact on our businesses (monument signs removed, equipment parked in front of buildings).

- An amendment to the code is requested in order to provide the Director of Community Development authority, at the Director's sole discretion, to administratively allow a banner to remain past the 14-day period for a business that fronts a roadway that is under construction. The roadway construction must be a project under construction for 6 months or longer and a project overseen by the city, Georgia Department of Transportation or Fulton County (not private development).
- Multi-tenant properties would only be allowed a single banner and if banners are not maintained in good condition, removal would be required.
- Director Cook shared that we cannot dictate what is said/verbiage on the banner.
- Proposed amendment language is attached hereto as "Exhibit A."
- City Attorney, Molly Esswein, read the ordinance title aloud.

Public Comment:

- There were no public comments.

City Council Discussion:

- Council Member Mitchell asked if it the construction period could be reduced to three (3) months.
- ❖ Mayor Pro Tem Merkel offered a motion to approve PH-22-10 / Unified Development Code (UDC) Text Amendment – Banner Signs – Public Hearing and First Reading.
 - Council Member DeRito seconded the motion.
 - The motion was approved unanimously (5-0).

VII. NEW BUSINESS

A. Citywide Security Systems: Badge Access Systems

- Director of Public Safety, John Robison, came forward to present this item.
- Staff is recommending that Mayor and Council award a contract for replacement/expansion of the city's badge reader system to NetPlanner Systems Inc. under the terms of GA State Contract #99999-SPD0000172-12 in an amount totaling \$254,808.36 and authorize the Mayor to execute all necessary documents. Included in this request is a reallocation of \$47,549 from the non-allocated reserve account within the Capital Project Fund.
- The FY 2023 capital budget included funding totaling \$220,000 for a refresh of the badge reader system, including the cost to remove and replace existing obsolete access control hardware within city buildings. The current system's electronic hardware is no longer manufactured, and replacement parts are no longer available.
- The project scope as proposed will upgrade the existing system, add additional control points to some buildings (not currently serviced), and add improved security to information technology infrastructure. Specifically, the 2023 funding request covers the

refresh/upgrade of existing equipment, and staff is requesting additional funding to cover the expansion of the badge reader system to multiple facilities that currently do not have a badge reader system and a 5% contingency to cover incidentals (supplies/materials).

Public Comment:

- There were no public comments.
- ❖ Council Member Will offered a motion to approve the award of a contract for replacement/expansion of the city's badge reader system to NetPlanner Systems Inc. under the terms of GA State Contract #99999-SPD0000172-12 in an amount totaling \$254,808.36 and authorize the Mayor to execute all necessary documents. Included in this request is a reallocation of \$47,549 from the non-allocated reserve account within the Capital Project Fund.
 - Council Member Mitchell seconded the motion.
 - The motion was approved unanimously (5-0).

B. Acceptance of the 2022 Fulton County Arts & Culture Grant Award

- Director of Recreation, Parks, and Cultural Services, Morgan Rodgers, came forward to present this item.
- Council Member Will left the meeting and abstained from this item, as his business is one that has applied to be a part of the Music Match program the past and may again in the future.
- Staff is recommending that Mayor and Council approve the acceptance of the 2022 Fulton County Arts & Culture Grant, with a matching contribution from the City of Alpharetta not to exceed \$15,000 and authorize the Mayor to execute all necessary documents.
- The Fulton County Arts & Culture Grant has been awarded to the City of Alpharetta in varying amounts for four consecutive years beginning in 2019. This year, the City has been awarded a \$15,000 Fulton County Arts & Culture Grant. The grant has a requirement for a \$15,000 match from the City of Alpharetta, which can be comprised of cash and in-kind services. \$15,000 City of Alpharetta Grant Match (Recreation, Parks, and Cultural Services has \$10,500 budgeted for this grant award and will contribute \$4,500 of city staff program hours to satisfy the match requirements).
- Traditionally, the City has used this grant to help fund the Alpharetta Music Match program. The Alpharetta Music Match program is part of the larger initiative, *Alpharetta Music City* and provides live music performances throughout the year in the City of Alpharetta, serving North Fulton residents and visitors. The City of

Alpharetta, Arts Alpharetta, Alpharetta Convention & Visitors Bureau, and Alpharetta Business Association promote the Music Match program.

- If this award acceptance is approved, the Fulton County Arts & Culture Grant will help fund approximately fifty (50) Live Music Match Performances in Alpharetta. The actual number of performances varies based on the cost of each performing artist's fees. In 2021, there were sixty-four (64) total music performances. Additionally, in 2021 and 2022, the Wire & Wood Songwriter's Festival utilized the Music Match Program to give businesses the opportunity to participate in the festival line-up.

Public Comment:

- There were no public comments.
- ❖ Mayor Pro Tem Merkel offered a motion to approve the acceptance of the 2022 Fulton County Arts & Culture Grant, with a matching contribution from the City of Alpharetta not to exceed \$15,000 and authorize the Mayor to execute all necessary documents.
 - Council Member Mitchell seconded the motion.
 - The motion was approved (4-0-1; as Council Member Will abstained from this item).
- Council Member Will rejoined the meeting once the Acceptance of the 2022 Fulton County Arts & Culture Grant Award item was voted upon and concluded.

VIII. PUBLIC COMMENT

- There were no public comments.

IX. REPORTS

- Mayor Pro Tem Merkel shared that unfortunately, Council Member Hipes was unable to attend tonight's meeting, but he wanted to pass along some positive remarks about the ribbon cutting ceremony for the Equestrian Center at Wills Park that occurred on Friday, September 16, 2022. Council Member Hipes was very proud of this event and the staff and others involved with making this happen.
- City Administrator, Chris Lagerbloom, shared that he may have a report after the conclusion of the Executive Session and asked the Mayor to hold this item open until after Executive Session.

X. EXECUTIVE SESSION

- ❖ Council Member DeRito offered a motion to recess to Executive Session.
 - Mayor Pro Tem Merkel seconded the motion.
 - The motion was approved unanimously (5-0).
- Mayor Gilvin recessed the meeting at 6:56 p.m.

- Mayor Gilvin reconvened the meeting at 7:26 p.m.

XI. REPORTS

- City Administrator, Chris Lagerbloom, shared the idea of discussing Judge Rich's report in regards to the City's Municipal Court and former Judge Barry Zimmerman at a future City Council meeting.
- Mayor Gilvin commented on the Local Option Sales Tax negotiations and Fulton County Commissioners discussing matters in a closed Executive Session.

XII. ADJOURNMENT

- ❖ Mayor Gilvin called for a vote to adjourn the meeting.
 - The City Council unanimously voted to adjourn the meeting (5-0).
- With there being no further items to consider or discuss, Mayor Gilvin adjourned the meeting at 7:34 p.m.

Respectfully submitted,



Lauren Shapiro, City Clerk

EXHIBIT A

SECTION 2.6 SIGNS¹

2.6.11 General provisions.

E. BANNERS. Banners require a permit and are permitted in all zoning districts pursuant to the following standards:

1. Banners shall be permitted for either one (1) fourteen (14) day period per calendar year per lot or two (2) seven (7) day periods per calendar year per lot. An individual banner permit may be divided into two (2) non-consecutive seven (7) day periods provided the dates are stated on the permit. However, in the case of lots which contain a shopping center (or strip shopping center) with multiple tenant spaces, each tenant space shall be allowed to erect or place a banner for either one (1) fourteen (14) day period per calendar year or two (2) seven (7) day periods per calendar year.

a. The Director may grant an extension of the time period set forth above for a commercial business when the business fronts a roadway that is under construction. In order to qualify for such an extension:

1. The subject roadway construction must be related to a project performed by the City, County or the Georgia Department of Transportation; and
2. The subject roadway construction is planned to continue for six (6) months or more following the date of the request for an extension; and
3. The subject roadway construction either:
 - a. Causes the removal of a monument sign; or
 - b. As determined in the discretion of the Director, disrupts the store frontage to the extent the site and/or business appears closed without the use of a banner.

Any extension granted under this subsection shall be limited to the duration of the subject roadway construction. Extensions granted by the Director may be revoked or limited at any time due to changes in the roadway construction or disruption of the store frontage as determined in the discretion of the Director. The Director may require removal or replacement of any banner placed pursuant to an extension at any time if the banner is not maintained in good condition as determined in the discretion of the Director.

2. In addition to the foregoing, banners shall be allowed on private property during an approved temporary use, as defined in Section 2.3.2 of the U.D.C., for the approved period of such temporary use, but not to exceed forty-five (45) days; provided, however, the placement of banners on lots during approved temporary uses shall not be permitted more than two (2) times per calendar year per lot. Any such banners shall be removed upon termination of the temporary use or within forty-five (45) days from the date it is first placed on the lot, whichever is first to occur. Upon removal, no banner shall be placed on the same lot for a period of sixty (60) days.
3. Banners shall not exceed 24 sq. ft. total area in size.

¹Editor's note(s)—Ord. No. 720 , § 2(Exh. A), adopted 2-22-2016, repealed former § 2.6 (2.6.1—2.6.14), and enacted a new § 2.6 as set out herein. The former § 2.6 pertained to similar subject matter and derived from the original codification and Ord. No. 713 , §§ 1—8, adopted Sept. 28, 2015.

-
4. Banners must either be free-standing or mounted to the wall of a tenant space or the lot's existing monument sign. If free-standing, the height of the banner shall not exceed five (5) [feet] above grade. If mounted to the wall of a tenant space, the width of the banner shall not exceed tenant frontage and shall not extend above the horizontal plane of the roof where the building wall and roof meet. If mounted to the lot's existing monument sign, the banner shall not extend beyond the sign face of the monument sign.
 5. Banners shall be erected with supports or other means so that they do not sag or become dilapidated.
- F. PLACEMENT OF SIGNS. Except within the Central Business District, all free-standing signs must be set back at least ten (10) ft. from the public right-of-way. Within the Central Business District, all free standing signs must be set back at least five (5) feet from the public right-of-way.
- G. CHANGEABLE COPY. Any monument sign permitted under this Ordinance may contain up to sixty-five percent (65%) changeable copy if the sign is located on a lot zoned and used (as its principal existing use) for an institutional, public or semi-public use and which includes an indoor public assembly place accommodating one hundred (100) or more persons.

(Ord. No. 720 , § 2(Exh. A), 2-22-2016)



STAFF REPORT

Submitting Department: Finance

Submitted By: Shawn Mitchell

Sponsored By:

Meeting Date: September 26, 2022

I. AGENDA ITEM TITLE: FINANCIAL MANAGEMENT REPORT: MONTH ENDING JULY 31, 2022
APPROVAL OF THE FINANCIAL MANAGEMENT REPORT FOR THE MONTH ENDING JULY 31, 2022

II. RECOMMENDATION:

Approve the Financial Management Reports for the month ending July 31, 2022 (period 1 of Fiscal Year 2023).

III. BUDGET IMPLICATIONS:

BUDGETED ITEM: NO

FISCAL IMPACT: NO

INCLUDED IN CURRENT FY CPTL BUDGET: NO

INCLUDED IN CURRENT FY OPRT. BUDGET: NO

TOTAL PROJECT COST:

APPROPRIATIONS:

ACCOUNT TITLE/NUMBER	DOLLAR AMOUNT
----------------------	---------------

EXTERNAL FUNDING SOURCES:

ACCOUNT TITLE/NUMBER	DOLLAR AMOUNT
----------------------	---------------

IV. REPORT IN BRIEF:

On a monthly basis, the Finance Department prepares detailed revenue and expenditure statements for all city operating funds (including prior-year comparisons for the General Fund).

In addition, this report includes:

1. Detailed capital project report including life-to-date activity;
2. Payments \$5,000 and greater; and
3. Purchase orders with an estimated cost between \$5,000 and \$50,000.

V. ALTERNATIVES:

VI. ATTACHMENTS:

FY 2023 FMR (1-July)

Financial Management Reports



**for the month ending
July 31, 2022
(period 1 of 12 – unaudited)**

Please visit the Financial Transparency Portal for additional information including audited financial statements, adopted budgets, and automated tools aimed at simplifying access to the City's financial data.

<https://www.alpharetta.ga.us/government/departments/finance/transparency-portal>

Financial Management Reports

Fiscal Year 2023

Table of Contents

Performance Dashboard	1
Transmittal Letter	2
General Fund	5
Revenue Summary and Collection Comparison	6
Expenditure Summary by Department	8
Expenditure Summary by Category	9
Grant and Capital Funds	10
Grant Funds	11
Capital Funds	15
Special Revenue Funds (w/capital projects)	26
Other Reports	29
Payments \$5,000 and Greater	30
PO's between \$5,000 and \$50,000	32
GAAP Financial Statements (Governmental/Enterprise Funds)	34
Alpharetta Development Authority	40
Revenue & Expenditure Report	41
GAAP Financial Statements	43
Republic Services	45
Accountability and Performance Dashboards	46-47



CITY OF ALPHARETTA

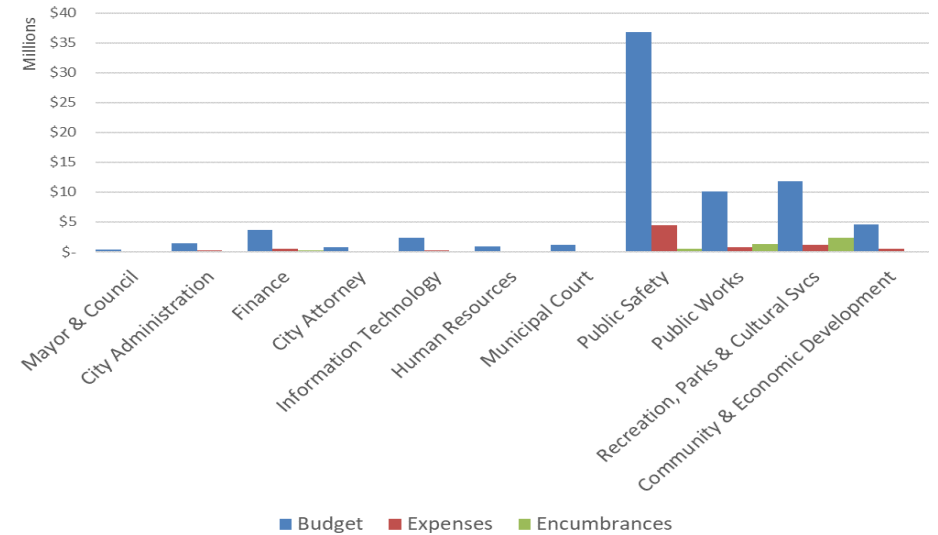
Financial Management Reports
Performance Dashboard
For the month ended July 31, 2022

LEGEND	
↑	Positive
↔	Neutral
↓	Negative

GENERAL FUND DETAIL

Revenues	Performance Status	Forecasted Gain/Loss
Top-10		
Property Taxes (incl. Motor Vehicle taxes)	↑	\$800,000
Local Option Sales Tax	↑	\$1,575,000
Franchise Tax	↔	\$0
Insurance Premium Tax	↔	\$0
Alcohol Beverage Excise Tax	↔	\$0
Building Permit Fees	↔	\$0
Business and Occupational Tax	↔	\$0
Court/Traffic Fines	↔	\$0
Recreation/Special Event Fees	↔	\$1,275
Hotel/Motel Tax (City portion)	↑	\$150,000
Other Revenues	↔	\$16,873
Revenue Gain: \$2.5M (3%)		Expenditure Gain: \$2.2M (3%)
Projected Fund Balance for Capital (FY 2025):		\$4.7M
Recurring Annual Capital Needs:		\$15M
Recurring Capital Contribution (FY 2025):		\$10.3M (Goal \$7.5M)

Departmental Budget Snapshot



FUND SYNOPSIS

	Revenue	Expenses	Non-Allocated
General Fund (1)	↑	↑	\$774,321
Special Revenue Funds			
Confiscated Assets Fund (DEA)	↔	↔	\$103,901
Confiscated Assets Fund (State)	↔	↔	\$0
Emergency 911 Fund (1)	↔	↔	\$96,224
Impact Fee Fund	↔	↔	\$958,471
Hotel/Motel Fund (1)	↑	↑	\$417,821
Debt Service Fund	↑	↑	\$767,968
Proprietary Funds			
Solid Waste Fund (2)	↔	↔	\$0
Risk Management Fund	↔	↔	\$1,434,177
Medical Insurance Fund	↔	↔	(\$633,196)

	Non-Allocated
Grant Funds	
Operating Grant Fund (3)	\$23,377
Capital Grant Fund (3)	(\$9,179)
Capital Project Funds	
Capital Project Fund (3)	\$3,227,912
Stormwater Capital Fund	\$72,863
Series 2016 Bond Fund (PW/Parks)	\$117,682
Series 2022 Bond Fund (Parks)	\$62,055
TSPLOST Capital Fund	\$863,446
TSPLOST 2 Capital Fund	\$0
American Rescue Plan Act Capital Fund	\$0
Development Authority Fund	\$64,551

BOND RATING

AAA

strongest rating available

EMERGENCY RESERVE

General Fund

\$19.7M est. (25%)

Emergency 911 Fund

\$1.25M est. (25%)

Sanitation Fund

\$144K est. (2%)

rate adj. improving reserve

Please Note: Current year revenue in excess of budgeted amounts may be available to augment Non-Allocated balances upon City Council approval (e.g. Impact Fee Fund collections).

(1) General Fund value represents Contingency balance. Hotel/Motel Fund value represents Debt Service Reserve (target is \$1.5 million). Other Funds represents amounts in excess of the 25% fund balance target.

(2) Solid Waste Fund operational trends will remain neutral despite the recent rate adjustment as it will take multiple years to replenish the fund balance target.

(3) Does not include amounts currently set aside for matches on active grant applications.



2 PARK PLAZA
ALPHARETTA, GA 30009
PHONE: 678.297.6000
WWW.ALPHARETTA.GA.US

TO: HONORABLE MAYOR AND CITY COUNCIL MEMBERS

FROM: THOMAS G. HARRIS, FINANCE DIRECTOR *TH*

DATE: SEPTEMBER 26, 2022

RE: FINANCIAL MANAGEMENT REPORTS AS OF JULY 31, 2022

The documents contained herein represent the financial management reports for the City of Alpharetta ("city") as of the period ending July 31, 2022.

The Finance Department is currently in the process of closing the accounting books for Fiscal Year 2022 (FY 2022). The figures represented herein are subject to change in accordance with accounting entries made during the closing process.

General Fund

Revenue: The following section pertains to information detailed in the attached Revenue Summary and Collection Comparison report. FY 2023 revenues are budgeted at \$79 million (net of Carryforward Fund Balance totaling \$13 million). As of July 31, 2022, actual revenue collections total 6% or \$5 million. Trends (property digest valuations and collection trends) indicate a net gain over budget of \$2.5 million with the detail as follows:

• Property Taxes:	\$ 800,000
• LOST:	2,575,000
• Hotel Taxes:	150,000
• Other:	<u>18,148</u>
Estimated Gain:	\$ 2,543,148 (rounded)

Revenue collection percentages are typically low for the first several months of the fiscal year due to various factors including: (a) property tax billings mailed in October that carry a December due date; and (b) accrual entries aimed at ensuring the city's revenues accurately reflect the period in which they were earned.

The preliminary digest for FY 2023, as provided by the Fulton County Tax Commissioner, currently totals \$6.1 billion (net of all exemptions/motor vehicle values) and represents growth of 5.7%, or \$330 million, over the FY 2022 digest. This growth is made up of reassessments (\$211 million) and new construction (\$119 million).

This digest figure will be reduced through property tax appeals, but the city will not know the full extent until appeal data is provided by the Fulton County Tax Commissioner. As it is still early, the budgetary estimate for FY

MAYOR
JIM GILVIN

MAYOR PRO TEM
DAN MERKEL

COUNCIL MEMBERS
JASON BINDER
DOUGLAS J. DERITO
JOHN HIPES
DONALD F. MITCHELL
BRIAN WILL

CITY
ADMINISTRATOR
ROBERT J. REGUS

2023 property tax collections will be set at \$27.1 million (\$800,000 growth over budget) pending collection data and appeal write-down trends.

Local Option Sales Tax collections are continuing their strong trends and conservative estimates for FY 2023 total \$20.5 million which is \$1.6 million greater than budget.

Hotel/Motel tax collections is discussed within the Special Revenue Funds section of this letter.

Expenditures: The following section pertains to information detailed in the attached Expenditure Summary by Department (expenditure rollup by department) and Expenditure Summary by Category (expenditure rollup by account) reports. As of July 31, 2022, city departments (not including General Government¹) have encumbered and expensed 17%, or \$12.8 million, of their FY 2023 budget appropriations.

Contingency: The General Fund contingency balance totals \$754,692.

Other Funds

The following section references information included within the attached Performance Dashboard, Grant and Capital Funds Detail Reports, GAAP Financial Statements, etc.

Operating Grant Fund (Fund 220): Unspent/unencumbered project appropriations total \$172,409. Remaining appropriations are set aside for grant matches (\$27,408) and a non-allocated reserve (\$23,377).

Capital Grants Fund (Fund 340): Unspent/unencumbered project appropriations total \$2.6 million.

General Capital Project Fund (Fund 301): Unspent/unencumbered project appropriations total \$15 million. Remaining appropriations are set aside for a non-allocated reserve (\$3.2 million).

Stormwater Capital Fund (Fund 302): Unspent/unencumbered project appropriations total \$4.8 million. Remaining appropriations are set aside for a non-allocated reserve (\$72,863).

American Rescue Act Capital Fund (Fund 303): Unspent/unencumbered project appropriations total \$2.7 million.

Series 2016 Parks and Transportation Bond Fund (Fund 317): Unspent/unencumbered project appropriations total \$55,729. Remaining appropriations are set aside for a non-allocated reserve (\$117,682).

Series 2022 Parks Bond Fund (Fund 318): Unspent/unencumbered project appropriations total \$28.8 million. Remaining appropriations are set aside for a non-allocated reserve (\$62,055).

TSPLOST 1 Capital Project Fund (Fund 335): This fund accounts for collections under the Transportation Special Local Option Sales Tax (TSPLOST) that went into effect on April 1, 2017 and expired on March 31, 2022. Unspent/unencumbered project appropriations total \$34 million. Remaining appropriations are set aside for a non-allocated reserve (\$863,446).

TSPLOST 2 Capital Project Fund (Fund 336): This fund accounts for collections under the Transportation Special Local Option Sales Tax (TSPLOST) that went into effect on April 1, 2022. Appropriated funding totals \$51 million and represents Tier-1 project funding. Tier-1 projects

¹ General Government is utilized to account for non-operating transactions such as transfers-out to other city funds, contingency, etc.

are funded at 85% of forecasted revenue collections over the life of the 5-year tax. For comparison purposes, TSPLOST 1 collections have trended at over 90% of forecasted revenue collections.

Hotel/Motel Fund: FY 2023 revenues are budgeted at \$7.5 million (net of carryforward fund balance totaling \$974,971) with budgeted disbursements as follows: Alpharetta Convention & Visitor's Bureau (43.75% or \$3.3 million); Facilities (18.75% and a portion of the carryforward fund balance detailed above; \$1.4 million for debt service on the Series 2016 Convention Center Bonds; \$592,687 for eligible initiatives such as Equestrian Center and Wills Park Master Plan Improvements; with residual funding for bond/debt service reserve); and the city (37.5% or \$2.8 million).

Specifically, Debt Service Reserve funding (Convention Center Bonds) from the Facilities portion of the tax totals \$417,821. This reserve figure dipped below the \$1.5 million target level in 2019 due to the impact of the COVID-19 pandemic on the hospitality industry and is being replenished as revenues within the Fund continue strengthening.

Hotel tax collections is continuing its strong growth and conservative estimates for FY 2023 total \$7.9 million which is \$400,000 greater than budget. This estimate will likely be revised in future months if collection trends continue.

Solid Waste Fund: FY 2023 revenues are currently budgeted at \$6.1 million. As of July 31, 2022, the city has collected \$9,695. During the FY 2022 year-end close process, the 1st quarter advanced billing (est. at \$1.65 million) will be accrued to FY 2023 (increasing revenue collections).

Other Items

Council Member Stipend Activity Listing: The FY 2023 budget includes appropriations of \$7,200 for the Mayor and \$4,000 for each City Council Post and the available balances as of July 31, 2022 are as follows:

	Budget	Expenditures	Available Balance
Mayor: Jim Gilvin	\$ 7,200	\$ 63	\$ 7,137
Post #1: Donald Mitchell	\$ 4,000	\$ 0	\$ 4,000
Post #2: Brian Will	\$ 4,000	\$ 242	\$ 3,758
Post #3: Doug DeRito	\$ 4,000	\$ 0	\$ 4,000
Post #4: John Hipes	\$ 4,000	\$ 97	\$ 3,903
Post #5: Jason Binder	\$ 4,000	\$ 0	\$ 4,000
Post #6: Dan Merkel	\$ 4,000	\$ 0	\$ 4,000

Development Authority² (Component Reporting Unit)

As of July 31, 2022, the Development Authority has \$64,551 in available resources to support its main functions of promoting the public good and general welfare, trade, commerce, industry, general tax base and the employment opportunities available in the city.

² The Development Authority is a public corporation created and existing under the Constitution and laws of the State of Georgia and is governed by seven directors duly appointed by the Alpharetta City Council.



GENERAL FUND

Revenue Report



CITY OF ALPHARETTA
 Financial Management Reports
 General Fund (Unaudited)
Revenue Summary and Collection Comparison
 As of July 31, 2022

	Current Fiscal Year					Prior Fiscal Year		
	2023 Budget	2023 YTD	% Collected	2023 Estimated	Variance	2022 Actual	2022 YTD	% Collected
Top 10 Revenues:								
Property Taxes								
Current Year	\$ 26,300,000	\$ 17,710	0.1%	\$ 27,100,000	\$ 800,000	\$ 26,738,657	\$ -	0.0%
Delinquent	147,000	18,798	12.8%	147,000	-	112,993	(26,159)	-23.2%
Motor Vehicle Tax	55,000	6,813	12.4%	55,000	-	72,772	-	0.0%
Motor Vehicle Title Fee	3,000,000	281,766	9.4%	3,000,000	-	2,861,031	-	0.0%
Local Option Sales Tax	18,925,000	1,814,023	9.6%	20,500,000	1,575,000	18,740,105	-	0.0%
Franchise Tax	7,100,000	211,540	3.0%	7,100,000	-	6,344,475	(372,538)	-5.9%
Insurance Premium Tax	4,825,000	-	0.0%	4,825,000	-	4,759,402	-	0.0%
Alcohol Beverage Excise Tax	2,575,000	254,926	9.9%	2,575,000	-	2,493,880	1,167	0.0%
Building Permit Fees	1,850,000	638,492	34.5%	1,850,000	-	1,987,196	128,765	6.5%
Business and Occupational Tax	1,000,000	10,303	1.0%	1,000,000	-	1,051,720	22,951	2.2%
Court/Traffic Fines	2,370,000	367,989	15.5%	2,370,000	-	2,809,444	108,297	3.9%
Recreation/Special Event Fees	2,822,279	159,871	5.7%	2,823,554	1,275	2,558,547	210,214	8.2%
Hotel/Motel Tax (City portion)	2,812,500	333,115	11.8%	2,962,500	150,000	2,644,129	-	0.0%
subtotal	\$ 73,781,779	\$ 4,115,345	5.6%	\$ 76,308,054	\$ 2,526,275	\$ 73,174,351	\$ 72,696	0.1%
Other Revenues	5,000,943	777,186	15.5%	5,017,816	16,873	4,762,906	158,852	3.3%
Total Revenues	\$ 78,782,722	\$ 4,892,531	6.2%	\$ 81,325,870	\$ 2,543,148	\$ 77,937,257	\$ 231,548	0.3%
Carryforward Fund Balance	12,639,800							



GENERAL FUND

Expenditure Reports



CITY OF ALPHARETTA
 Financial Management Reports
 General Fund (unaudited)
Expenditure Summary by Department
 As of July 31, 2022

Expenditures by Department:

	Current Fiscal Year						Prior Fiscal Year		
	2023 Budget	2023 Encumbrances	2023 Exp. (YTD)	Funds Available	% Enc./Exp.	% Exp.	2022 Exp. (Total)	2022 Exp. (YTD)	% Exp.
Mayor & Council	\$ 399,287	\$ 2,092	\$ 38,041	\$ 359,155	10.1%	9.5%	\$ 348,603	\$ 42,613	12.2%
City Administration	1,420,733	12,940	205,774	1,202,020	15.4%	14.5%	1,438,101	477,689	33.2%
Finance	3,698,826	207,447	564,108	2,927,271	20.9%	15.3%	3,436,956	605,446	17.6%
City Attorney	750,000	-	-	750,000	0.0%	0.0%	1,046,290	(2,290)	-0.2%
Information Technology	2,350,617	27,318	284,107	2,039,193	13.2%	12.1%	1,889,652	285,815	15.1%
Human Resources	855,513	45,761	71,995	737,757	13.8%	8.4%	604,968	93,264	15.4%
Municipal Court	1,148,200	49,653	102,621	995,926	13.3%	8.9%	1,077,497	84,847	7.9%
Public Safety	36,733,287	490,352	4,497,372	31,745,563	13.6%	12.2%	32,136,081	4,175,990	13.0%
Public Works	10,112,573	1,270,326	840,570	8,001,677	20.9%	8.3%	8,835,744	837,818	9.5%
Recreation, Parks & Cultural Svcs	11,796,631	2,414,783	1,120,806	8,261,042	30.0%	9.5%	10,265,061	1,041,638	10.1%
Community & Economic Development	4,630,115	62,312	536,814	4,030,988	12.9%	11.6%	4,071,650	498,262	12.2%
subtotal	\$ 73,895,782	\$ 4,582,983	\$ 8,262,209	\$ 61,050,590	17.4%	11.2%	\$ 65,150,602	\$ 8,141,091	12.5%
General Government:									
Insurance Premiums (Risk)	\$ 823,300	\$ -	\$ 68,608	\$ 754,692	8.3%	8.3%	\$ 779,750	\$ 64,979	8.3%
Gwinnett Tech Bond P&I	288,640	-	-	288,640	0.0%	0.0%	289,640	-	0.0%
Transfer(s) to other Funds	15,639,800	-	1,303,317	14,336,483	8.3%	8.3%	7,486,799	623,900	8.3%
Contingency	775,000	-	679	774,321	0.1%	0.1%	60,167	-	0.0%
subtotal	\$ 17,526,740	\$ -	\$ 1,372,604	\$ 16,154,136	7.8%	7.8%	\$ 8,616,356	\$ 688,879	8.0%
Total Expenditures	\$ 91,422,522	\$ 4,582,983	\$ 9,634,813	\$ 77,204,726	15.6%	10.5%	\$ 73,766,958	\$ 8,829,970	12.0%



CITY OF ALPHARETTA
Financial Management Reports
General Fund (unaudited)
Expenditure Summary by Category
As of July 31, 2022

	Current Fiscal Year						Prior Fiscal Year		
	2023 Budget	2023 Encumbrances	2023 Exp. (YTD)	Funds Available	% Enc./Exp.	% Exp.	2022 Exp. (Total)	2022 Exp. (YTD)	% Exp.
Expenditures by Category:									
Salaries & Benefits:									
(1) Regular Salaries	\$ 33,197,125	\$ -	\$ 2,056,048	\$ 31,141,077	6.2%	6.2%	\$ 28,833,638	\$ 1,831,399	6.4%
Overtime	2,191,950	-	199,548	1,992,402	9.1%	9.1%	2,452,865	180,354	7.4%
Group Insurance	10,081,080	-	1,152,037	8,929,043	11.4%	11.4%	8,067,559	1,170,282	14.5%
FICA and Social Security	2,705,978	-	161,527	2,544,451	6.0%	6.0%	2,277,379	143,569	6.3%
Defined Benefit Pension	2,869,712	-	2,869,712	-	100.0%	100.0%	2,818,660	2,818,660	100.0%
401(A) Retirement/Match	2,899,010	-	324,194	2,574,817	11.2%	11.2%	2,444,626	271,477	11.1%
(2) Other	1,535,153	-	728,615	806,538	47.5%	47.5%	1,402,233	635,741	45.3%
subtotal	\$ 55,480,008	\$ -	\$ 7,491,680	\$ 47,988,328	13.5%	13.5%	\$ 48,296,961	\$ 7,051,482	14.6%
Maintenance & Operations:									
Professional Services	\$ 2,839,142	\$ 872,693	\$ 206,671	\$ 1,759,778	38.0%	7.3%	\$ 2,839,655	\$ 422,846	14.9%
Legal Services	750,000	-	-	750,000	0.0%	0.0%	1,046,290	(2,290)	-0.2%
Vehicle Fuel/Maintenance	1,065,060	-	83,217	981,843	7.8%	7.8%	1,224,831	76,648	6.3%
Maintenance Contracts	3,705,288	2,592,083	68,973	1,044,232	71.8%	1.9%	3,005,871	97,175	3.2%
IT Professional Services	2,433,408	696,466	176,985	1,559,957	35.9%	7.3%	1,962,502	274,732	14.0%
General Supplies	967,951	130,451	41,397	796,103	17.8%	4.3%	893,611	63,690	7.1%
Utilities	2,900,691	-	21,511	2,879,180	0.7%	0.7%	2,748,597	2,503	0.1%
Insurance Premiums (Risk)	823,300	-	68,608	754,692	8.3%	8.3%	779,750	64,979	8.3%
Other	3,058,926	291,290	171,775	2,595,861	15.1%	5.6%	2,454,720	154,305	6.3%
subtotal	\$ 18,543,766	\$ 4,582,983	\$ 839,137	\$ 13,121,646	29.2%	4.5%	\$ 16,955,828	\$ 1,154,588	6.8%
Capital:									
OSSI/Fire Truck Leases	\$ 659,858	\$ -	\$ -	\$ 659,858	0.0%	0.0%	\$ 675,893	\$ -	0.0%
Other	35,450	-	-	35,450	0.0%	0.0%	1,671	-	0.0%
subtotal	\$ 695,308	\$ -	\$ -	\$ 695,308	0.0%	0.0%	\$ 677,563	\$ -	0.0%
General Government:									
Gwinnett Tech Bond P&I	\$ 288,640	\$ -	\$ -	\$ 288,640	0.0%	0.0%	\$ 289,640	\$ -	0.0%
Transfer(s) to other Funds	15,639,800	-	1,303,317	14,336,483	8.3%	8.3%	7,486,799	623,900	8.3%
Contingency	775,000	-	679	774,321	0.1%	0.1%	60,167	-	0.0%
subtotal	\$ 16,703,440	\$ -	\$ 1,303,996	\$ 15,399,444	7.8%	7.8%	\$ 7,836,606	\$ 623,900	8.0%
Total Expenditures	\$ 91,422,522	\$ 4,582,983	\$ 9,634,813	\$ 77,204,726	15.6%	10.5%	\$ 73,766,958	\$ 8,829,970	12.0%

Notes:

- (1) Includes the following components: regular salaries, holiday leave, temporary and seasonal salaries, and separation payout.
- (2) Includes the following components: workers compensation, educational programs, automobile allowance, tuition reimbursement, and employee service awards.



GRANT AND CAPITAL FUNDS

Revenue & Expenditure Reports



CITY OF ALPHARETTA
Financial Management Reports
Grant Funds
Operating Grant Fund Detail (Fund 220; life-to-date for active projects)
As of July 31, 2022

			Project Snapshot: FY2013 - FY2022		FY 2023					
Account #	Project		Total Project Authorization	Prior Year Actuals	Original Appropriation	Transfers / Adjustments	Revised Budget	Collections / Expenditures	Encumbrances	Available Budget
Revenues										
City Administration										
22013230-371000	C2100	MURAL ART PROJECT	15,915	15,915	\$ -	\$ -	\$ -	\$ -		\$ -
subtotal					\$ -	\$ -	\$ -	\$ -		\$ -
Public Safety										
22031150-331110	C1730	2017 BULLETPROOF VEST (DOJ)	13,179	12,462	\$ -	\$ 717	\$ 717			\$ 717
22031150-331110	C1831	2018 BULLETPROOF VEST (DOJ)	15,375	7,314	-	8,061	8,061			8,061
22031150-331110	C2018	2019 BULLETPROOF VEST (DOJ)	19,188	3,353	-	15,835	15,835			15,835
22031150-331110	C2059	2020 BULLETPROOF VEST (DOJ)	17,159	-	-	17,159	17,159			17,159
22031150-331110	C2115	2021 BULLETPROOF VEST (DOJ)	11,624	-	-	11,624	11,624			11,624
subtotal					\$ -	\$ 53,396	\$ 53,396	\$ -		\$ 53,396
Recreation, Parks & Cultural Services										
22061150-347509	C2039	WIRE & WOOD (ACVB SPONSOR)	152,000	102,000	\$ -	\$ 50,000	\$ 50,000	\$ 50,000		\$ -
22061150-371000	C2212	PARKING PERMIT - FILM	4,000	4,000	-	-	-			-
22061150-336000	C2213	2021 CAMP HAPPY HEARTS	5,000	5,000	-	-	-			-
22061150-336000	C2215	FC ARTS & CULTURE	7,800	7,800	-	-	-			-
22061150-336001	C2234	ARTS CENTER (CERAMICS)	2,248	2,248	-	-	-			-
22061150-347509	C2239	NORTH PARK SOFTBALL TOURNEY	2,397	2,397	-	-	-			-
22061150-347509	C2240	TOWN GREEN CONCERTS	5,000	5,000	-	-	-			-
22061150-347509	C2241	WP PROMO (AMERIS BANK AMP)	2,500	-	-	2,500	2,500	2,500		-
subtotal					\$ -	\$ 52,500	\$ 52,500	\$ 52,500		\$ -
General Government										
22090200-361000		INTEREST EARNINGS			\$ -	\$ -	\$ -	\$ 118		\$ (118)
22090200-362000		REALIZED GAIN/LOSS ON INVS			-	-	-	-		-
22090200-363000		UNREALIZED GAIN/LOSS			-	-	-	249		(249)
22090200-395000		CARRYFORWARD FUND BALANCE			-	119,627	119,627	-		119,627
subtotal					\$ -	\$ 119,627	\$ 119,627	\$ 368		\$ 119,259
Total					\$ -	\$ 225,523	\$ 225,523	\$ 52,868		\$ 172,655



CITY OF ALPHARETTA

Financial Management Reports

Grant Funds

Operating Grant Fund Detail (Fund 220; life-to-date for active projects)

As of July 31, 2022

Account #Project			Project Snapshot: FY2013 - FY2022		FY 2023					Available Budget
			Total Project Authorization	Prior Year Actuals	Original Appropriation	Transfers / Adjustments	Revised Budget	Collections / Expenditures	Encumbrances	
Expenditures										
City Administration										
22013230-521200	C2100	MURAL ART PROJECT	17,215	2,800	\$ -	\$ 14,415	\$ 14,415	\$ -	\$ -	\$ 14,415
subtotal					\$ -	\$ 14,415	\$ 14,415	\$ -	\$ -	\$ 14,415
Public Safety										
22031150-542100	C1730	2017 BULLETPROOF VEST (DOJ)	26,357	24,925	\$ -	\$ 1,432	\$ 1,432	\$ -	\$ -	\$ 1,432
22031150-542100	C1831	2018 BULLETPROOF VEST (DOJ)	30,751	16,675	-	14,076	14,076	-	-	14,076
22031150-542100	C2018	2019 BULLETPROOF VEST (DOJ)	30,016	12,280	-	17,736	17,736	-	-	17,736
22031150-542100	C2059	2020 BULLETPROOF VEST (DOJ)	38,964	4,646	-	34,318	34,318	-	-	34,318
22031150-542100	C2115	2021 BULLETPROOF VEST (DOJ)	23,248	-	-	23,248	23,248	-	-	23,248
subtotal					\$ -	\$ 90,810	\$ 90,810	\$ -	\$ -	\$ 90,810
Recreation, Parks & Cultural Services										
22061159-521200	C2039	WIRE & WOOD (ACVB SPONSOR)	100,000	50,000	\$ -	\$ 50,000	\$ 50,000	\$ -	\$ -	\$ 50,000
22061150-531100	C2101	SPECIAL NEEDS EXPO / EVENT	1,018	-	-	1,018	1,018	-	-	1,018
22061150-531100	C2102	FULTON GOLDEN GAMES	3,630	-	-	3,630	3,630	-	-	3,630
22061150-531100	C2212	PARKING PERMIT - FILM	4,000	3,750	-	250	250	-	-	250
22061150-531100	C2213	2020 CAMP HAPPY HEARTS	5,000	2,671	-	2,329	2,329	-	2,329	-
22061150-531100	C2215	FC ARTS & CULTURE	7,800	6,056	-	1,744	1,744	-	-	1,744
22061150-531100	C2234	ARTS CENTER (CERAMICS)	2,249	1,604	-	645	645	-	-	645
22061150-523300	C2239	NORTH PARK SOFTBALL TOURNEY	2,397	-	-	2,397	2,397	-	-	2,397
22061150-523300	C2240	TOWN GREEN CONCERTS	5,000	-	-	5,000	5,000	-	-	5,000
22061150-523300	C2241	WP PROMO (AMERIS BANK AMP)	4,998	2,498	-	2,500	2,500	-	-	2,500
subtotal					\$ -	\$ 69,513	\$ 69,513	\$ -	\$ 2,329	\$ 67,184
Non-Allocated										
22090200-579000		CONTINGENCY			\$ -	\$ 23,377	\$ 23,377	\$ -	\$ -	\$ 23,377
22090200-579011		MATCH (GRANTS UNDER REVIEW)			-	27,408	27,408	-	-	27,408
subtotal					\$ -	\$ 50,785	\$ 50,785	\$ -	\$ -	\$ 50,785
Total					\$ -	\$ 225,523	\$ 225,523	\$ -	\$ 2,329	\$ 223,194



CITY OF ALPHARETTA
Financial Management Reports
Grant Funds
Capital Grant Fund Detail (Fund 340; life-to-date for active projects)
As of July 31, 2022

			Project Snapshot: FY2013 - FY2022		FY 2023					
			Total Project Authorization	Prior Year Actuals	Original Appropriation	Transfers / Adjustments	Revised Budget	Collections / Expenditures	Encumbrances	Available Budget
Account #	Project									
Revenue										
Public Safety										
34031150-331350	C2235	CRABAPPLE TRAINING FACILITY	46,130	-	\$ -	\$ 46,130	\$ 46,130	\$ -		\$ 46,130
34034450-331150	C2244	2020 HOMELAND SECURITY GRANT	45,900	-	-	45,900	45,900	-		45,900
34031150-331150	C2246	2021 HOMELAND SECURITY GRANT	22,500	-	-	22,500	22,500	-		22,500
subtotal					\$ -	\$ 114,530	\$ 114,530	\$ -		\$ 114,530
Public Works										
34041100-334310	C1219	MILLING AND RESURFACING (LMIG)	5,234,146	5,234,146	\$ -	\$ -	\$ -	\$ -		\$ -
34041100-331150	C2242	NORTHPOINT ALPHALINK (ARC/LCI)	1,000,000	-	-	1,000,000	1,000,000	-		1,000,000
34041100-331350	GRANT	ALPHALOOP (LANDWATER)	500,000	-	-	500,000	500,000	-		500,000
subtotal					\$ -	\$ 1,500,000	\$ 1,500,000	\$ -		\$ 1,500,000
Community Development										
34074150-331350	C2107	NORTH POINT PKWY IMP	1,667,001	509,141	\$ -	\$ 1,157,860	\$ 1,157,860	\$ 69,387		\$ 1,088,474
34074150-331150	C2114	S MAIN ST ARC STUDY	160,000	17,160	-	142,840	142,840	17,640		125,200
subtotal					\$ -	\$ 1,300,700	\$ 1,300,700	\$ 87,027		\$ 1,213,674
General Government										
34090200-361000		INTEREST EARNINGS			\$ -	\$ -	\$ -	102		\$ (102)
34090200-362000		REALIZED GAIN/LOSS ON INVS			-	-	-	-		-
34090200-363000		UNREALIZED GAIN/LOSS			-	-	-	214		(214)
34090200-395000		CARRYFORWARD FUND BALANCE			-	(69,782)	(69,782)	-		(69,782)
subtotal					\$ -	\$ (69,782)	\$ (69,782)	\$ 315		\$ (70,097)
Total					\$ -	\$ 2,845,448	\$ 2,845,448	\$ 87,342		\$ 2,758,106



CITY OF ALPHARETTA
Financial Management Reports
Grant Funds
Capital Grant Fund Detail (Fund 340; life-to-date for active projects)
As of July 31, 2022

				Project Snapshot: FY2013 - FY2022		FY 2023					
				Total Project Authorization	Prior Year Actuals	Original Appropriation	Transfers / Adjustments	Revised Budget	Collections / Expenditures		Encumbrances
Account #	Project										
Expenditures											
Public Safety											
34031150-542100	C2235	CRABAPPLE TRAINING FACILITY		46,130	46,130	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -
34031150-542100	C2244	HOMELAND SECURITY GRANT		45,900	-	-	45,900	45,900	16,500	27,600	1,800
34031150-542100	C2246	HOMELAND SECURITY GRANT		22,500	-	-	22,500	22,500	-	-	22,500
						\$ -	\$ 68,400	\$ 68,400	\$ 16,500	\$ 27,600	\$ 24,300
Public Works											
34041100-541410	C1215	STRIPING & SIGNAGE		185,325	185,325	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -
34041100-541410	C1219	MILLING AND RESURFACING (LMIG)		5,234,146	5,234,146	-	-	-	-	-	-
34041100-521200	C2242	NORTHPOINT ALPHALINK (ARC/LCI)		1,000,000	-	-	1,000,000	1,000,000	-	-	1,000,000
34041100-541420	C2305	ALPHALOOP (LANDWATER)		500,000	-	-	500,000	500,000	-	-	500,000
subtotal						\$ -	\$ 1,500,000	\$ 1,500,000	\$ -	\$ -	\$ 1,500,000
Community Development											
34074150-541410	C2107	NORTH POINT PKWY IMP		2,083,748	903,121	\$ -	\$ 1,180,627	\$ 1,180,627	\$ -	\$ 132,526	\$ 1,048,101
34074150-521200	C2114	S MAIN ST ARC STUDY		160,000	54,400	-	105,600	105,600	-	105,600	-
subtotal						\$ -	\$ 1,286,227	\$ 1,286,227	\$ -	\$ 238,126	\$ 1,048,101
Non-Allocated											
34090200-579000		CONTINGENCY				\$ -	\$ (9,179)	\$ (9,179)	\$ -	\$ -	\$ (9,179)
subtotal						\$ -	\$ (9,179)	\$ (9,179)	\$ -	\$ -	\$ (9,179)
Total						\$ -	\$ 2,845,448	\$ 2,845,448	\$ 16,500	\$ 265,726	\$ 2,563,222



CITY OF ALPHARETTA
 Financial Management Reports
 Capital Project Funds
General Capital Project Fund Detail (Fund 301; life-to-date for active projects)
 As of July 31, 2022

			Project Snapshot: FY2013 - FY2022		FY 2023					
			Total Project Authorization	Prior Year Actuals	Original Appropriation	Transfers / Adjustments	Revised Budget	Collections / Expenditures	Encumbrances	Available Budget
Account #	Project									
Revenue										
30141100-336000	C1410	RUCKER RD WATERLINE	1,562,604	1,459,845	\$ -	\$ 102,759	\$ 102,759	\$ -		\$ 102,759
30141100-336000	C1702	KIMBALL BR RD IMPROVEMENTS	6,146,785	5,508,534	-	638,251	638,251	35,984		602,267
30141100-371000	C2113	ENCORE GREENWAY GATEWAY	430,000	-	-	430,000	430,000	-		430,000
30141100-336000	C2238	DAVIS DR. WATER (COUNTY)	364,488	-	-	364,488	364,488	-		364,488
30161150-371000	C1929	COMM AG PROGRAM	50,135	50,135	-	-	-	709		(709)
30161150-371000	C2010	MEMORIAL-PARK ENHANCEMENTS	11,100	11,100	-	-	-	3,000		(3,000)
30174150-337000	C0910	TREE REPLACEMENT FUND (CONTRIBUTION)	467,450	467,450	-	-	-	2,100		(2,100)
30113230-336000	C0924	ECONOMIC DEVELOPMENT PLAN	37,500	-	-	37,500	37,500	-		37,500
30176100-371000	C1712	ALPHALOOP (ABC)	689,187	439,981	-	249,206	249,206	-		249,206
		subtotal			\$ -	\$ 1,822,204	\$ 1,822,204	\$ 41,793		\$ 1,780,411
Non-Departmental										
30190200-395000		CARRYFORWARD FUND BALANCE			\$ 2,500,000	\$ 5,817,846	\$ 8,317,846	\$ -		\$ 8,317,846
30190200-391100		TRANSFER-IN FROM THE GENERAL FUND			11,439,800	-	11,439,800	953,317		10,486,483
30190200-363000		UNREALIZED GAIN/LOSS INV			-	-	-	18,595		(18,595)
30190200-389000		MISCELLANEOUS REVENUE			-	-	-	-		-
30190200-361000		INTEREST EARNINGS			155,000	-	155,000	8,834		146,166
		subtotal			\$ 14,094,800	\$ 5,817,846	\$ 19,912,646	\$ 980,746		\$ 18,931,900
		Total			\$ 14,094,800	\$ 7,640,050	\$ 21,734,850	\$ 1,022,539		\$ 20,712,311
Expenditures										
Administration										
30113230-542400	C1404	WEBSITE UPGRADE	145,000	-	\$ 145,000	\$ -	\$ 145,000	\$ -	\$ -	\$ 145,000
30113230-544100	C2105	BUSINESS RECOVERY PROGRAM	150,000	50,000	-	100,000	100,000	-	-	100,000
		subtotal			\$ 145,000	\$ 100,000	\$ 245,000	\$ -	\$ -	\$ 245,000



CITY OF ALPHARETTA
 Financial Management Reports
 Capital Project Funds
General Capital Project Fund Detail (Fund 301; life-to-date for active projects)
 As of July 31, 2022

Account #		Project		Project Snapshot: FY2013 - FY2022		FY 2023					Available Budget
				Total Project Authorization	Prior Year Actuals	Original Appropriation	Transfers / Adjustments	Revised Budget	Collections / Expenditures	Encumbrances	
Finance				363,044	354,302						
30115150-542400	C1141	TYLER ERP SYSTEM				\$ -	\$ 8,742	\$ 8,742	\$ 5,362	\$ 3,380	
		subtotal				\$ -	\$ 8,742	\$ 8,742	\$ -	\$ 5,362	\$ 3,380
Information Technology				300,002	189,138						
30117400-542400	C0900	CISCO DATA NETWORK				\$ -	\$ 110,864	\$ 110,864	\$ -	\$ 1,600	\$ 109,264
30117400-542400	C1000	GIS AERIAL MAPPING				-	1,717	1,717	233	1,484	1
30117400-542400	C1103	NETWORK AND VOIP				200,000	363,469	563,469	-	-	563,469
30117400-542400	C1312	BACKUP DATA STORAGE MGMT.				-	21,056	21,056	-	-	21,056
30117400-542400	C1313	TECHNOLOGY REPLACEMENT				250,000	270,782	520,782	368	23,752	496,662
30117400-542400	C1615	APP/DESKTOP VIRTUALIZATION				-	283,896	283,896		12,500	271,396
30117400-542400	C2201	CITY COUNCIL A/V REPLACEMENT				-	269,816	269,816	-	161,792	108,024
30117400-544200	C2300	BUSINESS CONTINUITY STUDY				50,000	-	50,000	-	-	50,000
		subtotal				\$ 500,000	\$ 1,321,600	\$ 1,821,600	\$ 601	\$ 201,128	\$ 1,619,871
Human Resources						72,500	-				
30118450-542400	C1222	RECORDS MANAGEMENT		\$ 72,500	\$ -			\$ 72,500	\$ -	\$ -	\$ 72,500
		subtotal		\$ 72,500	\$ -			\$ 72,500	\$ -	\$ -	\$ 72,500
Municipal Court				39,600	32,900						
30126550-542400	C1222	RECORDS MANAGEMENT				\$ -	\$ 6,700	\$ 6,700	\$ 6,700	\$ -	
		subtotal				\$ -	\$ 6,700	\$ 6,700	\$ -	\$ 6,700	\$ -
Public Safety				7,916,893	6,142,656						
30131150-542200	C1202	FLEET REPLACEMENT				\$ 1,375,000	\$ 399,237	\$ 1,774,237	\$ -	\$ 262,206	\$ 1,512,031
30131150-541300	C1229	PS ROOF REPAIR				300,000	(7,579)	292,421	-	-	292,421
30131150-542100	C1401	PS EQUIPMENT REPLACEMENT				263,000	110,343	373,343	1,089	104,964	267,290
30131150-541300	C1706	RAPSTC IMPROVEMENTS				-	318,836	318,836	-	102,143	216,693
30131150-542400	C2052	SECURITY SYSTEM REFRESH				220,000	3,025	223,025	-	-	223,025
30131150-542100	C2055	LICENSE PLATE READER PROGRAM				-	20,000	20,000	4,433	4,160	11,407
30131150-542100	C2207	LUCAS DEVICES				-	6,058	6,058	-	-	6,058
30131150-542100	C2235	CRABAPPLE TRAINING FACILITY				-	6,318	6,318	441	-	5,877



CITY OF ALPHARETTA
 Financial Management Reports
 Capital Project Funds
General Capital Project Fund Detail (Fund 301; life-to-date for active projects)
 As of July 31, 2022

Account #	Project	Project Snapshot: FY2013 - FY2022		FY 2023					Available Budget
		Total Project Authorization	Prior Year Actuals	Original Appropriation	Transfers / Adjustments	Revised Budget	Collections / Expenditures	Encumbrances	
30131150-542400	C2301 CAD/RECORDS MANAGEMENT SOFTWARE	2,250,000	-	2,250,000	-	2,250,000	-	-	2,250,000
30131150-542100	C2302 ALL TERRAIN VEHICLES	11,310	-	11,310	-	11,310	-	-	11,310
30131150-542100	C2303 2023 OP INITIATIVES EQUIPMENT	449,500	-	449,500	-	449,500	-	-	449,500
	subtotal			\$ 4,868,810	\$ 856,238	\$ 5,725,048	\$ 5,963	\$ 473,473	\$ 5,245,612
Public Works									
30141100-541410	C0041 TRAFFIC SIGNAL INTERCONNECT	279,781	275,044	\$ -	\$ 4,737	\$ 4,737	\$ -	\$ 3,810	\$ 927
30141100-541200	C0910 TREE REPLACEMENT FUND	1,626,301	1,404,067	-	222,234	222,234	-	218,811	3,423
30141100-541200	C1008 CEMETERY AUTHORITY-MAINTENANCE	479,543	207,186	-	272,357	272,357	-	11,991	260,366
30141100-541410	C1207 BRIDGE MAINTENANCE	665,212	377,330	200,000	87,882	287,882	-	-	287,882
30141100-541410	C1215 STRIPING & SIGNAGE	2,014,664	1,814,664	200,000	-	200,000	-	19,103	180,897
30141100-541410	C1217 TRAFFIC CALMING & INTERSECTION IMP	553,584	432,814	100,000	20,770	120,770	-	20,649	100,122
30141100-541410	C1218 TRAFFIC SIGNAL SYSTEM MAINTENANCE	804,267	691,872	100,000	12,395	112,395	9,895	14,297	88,203
30141100-541410	C1219 MILLING AND RESURFACING	23,174,573	21,564,565	1,000,000	610,008	1,610,008	1,471	256,657	1,351,881
30141100-541410	C1220 TRAFFIC CONTROL EQUIPMENT	987,078	887,078	100,000	-	100,000	3,369	-	96,631
30141100-541410	C1221 DESIGN SERVICES	943,300	794,459	75,000	73,841	148,841	2,290	-	146,551
30141100-542200	C1223 FLEET REPLACEMENT	1,469,452	1,091,468	195,000	182,984	377,984	42,975	182,789	152,220
30141100-541200	C1302 TREE PLANTING & LANDSCAPING IMP	1,222,771	817,220	100,000	305,551	405,551	-	254,025	151,526
30141100-542100	C1802 PW EQUIPMENT REPLACEMENT	217,373	173,446	36,000	7,927	43,927	-	-	43,927
30141100-541410	C1901 TRAFFIC RESPONSIVE SYSTEM MAINT	450,001	299,856	100,000	50,145	150,145	16,240	34,498	99,407
30141100-541300	C1902 FIRE STATION RENOVATIONS	510,003	419,519	75,000	15,484	90,484	-	4,461	86,023
30141100-541300	C1904 PW HQ RENOVATIONS	178,037	121,982	50,000	6,055	56,055	-	-	56,055
30141100-541300	C1905 GYM RENOVATIONS	35,000	-	35,000	-	35,000	-	-	35,000
30141100-541410	C1918 PEDESTRIAN SAFETY STUDY	381,115	296,115	85,000	-	85,000	-	-	85,000
30141100-541410	C1935 WINDWARD PKWY WEST IMPROVEMENTS	305,753	203,977	-	101,776	101,776	-	101,775	1
30141100-541300	C2003 HVAC REPLACEMENTS	292,002	227,797	62,000	2,205	64,205	-	-	64,205
30141100-541300	C2004 GENERATOR REPLACEMENTS	295,075	187,197	-	107,878	107,878	-	4,752	103,126
30141100-542400	C2026 TCC HARDWARE/SOFTWARE	170,001	77,836	50,000	42,165	92,165	451	4,738	86,976
30141100-541410	C2048 STREETLIGHT MAINTENANCE	269,079	104,108	80,000	84,971	164,971	638	42,720	121,614
30141100-541500	C2050 REC FACILITY MAINTENANCE	120,000	46,645	30,000	43,355	73,355	-	-	73,355



CITY OF ALPHARETTA
 Financial Management Reports
 Capital Project Funds
General Capital Project Fund Detail (Fund 301; life-to-date for active projects)
 As of July 31, 2022

Account #	Project	Project Snapshot: FY2013 - FY2022		FY 2023					Available Budget
		Total Project Authorization	Prior Year Actuals	Original Appropriation	Transfers / Adjustments	Revised Budget	Collections / Expenditures	Encumbrances	
30141100-541300	C2053 PARKING GARAGE MAINTENANCE	145,351	36,582	100,000	8,769	108,769	-	-	108,769
30141100-541410	C2113 ENCORE GREENWAY GATEWAY	430,000	19,456	-	410,544	410,544	-	410,544	0
30141100-544200	C2200 CITY TRASH RECEPTACLE SERVICE	100,001	39,159	50,000	10,842	60,842	-	3,472	57,370
30141100-541410	C2238 DAVIS DR WATER (COUNTY)	364,488	-	-	364,488	364,488	-	364,488	-
30141100-521200	C2242 NORTHPOINT ALPHALINK (ARC/LCI)	285,000	-	-	285,000	285,000	-	35,000	250,000
30141100-541420	C2305 ALPHALOOP (OMP - NORTHWINDS)	247,403	-	-	247,403	247,403	-	-	247,403
	subtotal			\$ 2,823,000	\$ 3,581,766	\$ 6,404,766	\$ 77,329	\$ 1,988,579	\$ 4,338,859
Recreation, Parks & Cultural Services									
30161150-541500	C0922 SYNTHETIC TURF REPLACEMENT	1,014,966	464,966	\$ 550,000	\$ -	\$ 550,000	\$ -	\$ -	\$ 550,000
30161150-541200	C1210 TREE REMOVAL			150,000	-	150,000	21,080	128,920	-
30161150-541500	C1221 DESIGN SERVICES	214,224	186,473	20,000	7,751	27,751	542	-	27,209
30161150-541300	C1229 FACILITY ROOF REPAIR	494,741	-	700,000	(205,259)	494,741	-	-	494,741
30161150-542200	C1232 FLEET	352,578	72,130	120,000	160,448	280,448	-	160,448	120,000
30161150-542100	C1402 RP EQUIPMENT REPLACEMENT	799,218	699,218	100,000	-	100,000	-	53,432	46,568
30161150-541500	C1424 WILL PARK POOL EXPANSION	59,000	51,200	-	7,800	7,800	-	-	7,800
30161150-541500	C1520 WILLS PARK TENNIS CT RESURFACE	48,983	48,918	-	65	65	-	65	-
30113230-544200	C1527 VETERANS MEMORIAL	105,667	75,806	-	29,861	29,861	-	-	29,861
30161150-541500	C1614 THE STORIES PROJECT	85,000	31,065	35,000	18,935	53,935	-	-	53,935
30161150-541510	C1636 GREENWAY REPAIR AND MAINTENANCE	907,169	370,594	155,000	381,575	536,575	-	26,280	510,295
30161150-541500	C1804 PARK REPAIRS/IMPROVEMENTS	830,877	521,159	300,000	9,718	309,718	17,420	179,800	112,498
30161150-541500	C1806 PARKS PLAYGROUND EQUIPMENT	490,721	277,238	150,000	63,483	213,483	-	-	213,483
30161150-544100	C1807 PUBLIC ARTS PROGRAM	231,000	170,000	45,000	16,000	61,000	-	-	61,000
30161150-541500	C1926 NORTHSIDE MOU (PARKS)	146,303	117,657	-	28,646	28,646	-	-	28,646
30161150-541500	C1929 COMMUNITY AGRICULTURE PROGRAM	50,139	35,170	-	14,969	14,969	5,212	-	9,757
30161150-541500	C2010 PARK ENHANCEMENTS	598,179	465,437	125,000	7,742	132,742	4,002	8,372	120,368
30161150-541500	C2030 TOWN GREEN IMPROVEMENTS	250,000	-	250,000	-	250,000	-	-	250,000
30161150-541500	C2031 INNOVATION ACADEMY IGA	250,000	249,638	-	362	362	354	-	8
30161150-541500	C2051 FOUNTAIN MAINTENANCE	36,306	27,309	-	8,997	8,997	-	-	8,997
30161150-541500	C2202 ATHELETIC COURTS RESURFACING	98,433	58,433	40,000	-	40,000	-	-	40,000
30161150-541500	C2245 WILL PARK MAINTENANCE FACILITY	116,001	766	-	115,235	115,235	-	49,927	65,308
30161150-541500	C2304 PARK WOOD POLE REPLACEMENT	200,000	-	200,000	-	200,000	-	-	200,000
	subtotal			\$ 2,940,000	\$ 666,328	\$ 3,606,328	\$ 48,610	\$ 607,243	\$ 2,950,475



CITY OF ALPHARETTA
 Financial Management Reports
 Capital Project Funds
General Capital Project Fund Detail (Fund 301; life-to-date for active projects)
 As of July 31, 2022

			Project Snapshot: FY2013 - FY2022		FY 2023					
			Total Project Authorization	Prior Year Actuals	Original Appropriation	Transfers / Adjustments	Revised Budget	Collections / Expenditures	Encumbrances	Available Budget
Account #	Project									
Community Development										
30174150-544100	C0019	DOWNTOWN PARKING FUND	576,749	297,748	\$ -	\$ 279,001	\$ 279,001	\$ -	\$ -	\$ 279,001
30174150-544100	C0924	ECONOMIC DEVELOPMENT PLAN	107,640	62,500	-	45,140	45,140		45,140	-
30174150-544200	C1300	CITY ECON DEVELOPMENT TOOLKIT	263,260	202,010	-	61,250	61,250	-	-	61,250
30174150-542200	C1433	FLEET REPLACEMENT	60,000	-	60,000	-	60,000	-	-	60,000
30174150-541410	C1603	DESIGN SERVICES	476,003	370,377	40,000	65,626	105,626	-	33,643	71,983
30174150-541410	C2107	NORTH POINT PARKWAY IMPROVEMENTS	78,500	52,670	-	25,830	25,830	-	25,830	0
30174150-542400	C2111	COMMUNITY DEVELOPMENT EQUIPMENT	21,000	7,993	-	13,007	13,007	-	-	13,007
30174150-521200	C2114	S MAIN ST ARC STUDY	40,000	13,600	-	26,400	26,400	-	26,400	-
		subtotal			\$ 100,000	\$ 516,254	\$ 616,254	\$ -	\$ 131,013	\$ 485,241
Non-Departmental										
30190200-579000		NON-ALLOCATED			\$ 2,645,490	\$ 582,422	\$ 3,227,912	\$ -	\$ -	\$ 3,227,912
30190200-579011		GRANTS UNDER REVIEW			-	-	-	-	-	-
30190200-521200		PROFESSIONAL SERVICES			-	-	-	-	-	-
		subtotal			\$ 2,645,490	\$ 582,422	\$ 3,227,912	\$ -	\$ -	\$ 3,227,912
		Total			\$ 14,094,800	\$ 7,640,050	\$ 21,734,850	\$ 132,502	\$ 3,413,498	18,188,850



CITY OF ALPHARETTA
 Financial Management Reports
 Capital Project Funds
Stormwater Capital Fund Detail (Fund 302; life-to-date for all projects)
 As of July 31, 2022

Account #	Project	Project Snapshot: FY2017 - FY2022		FY 2023					
		Total Project Authorization	Prior Year Actuals	Original Appropriation	Transfers / Adjustments	Revised Budget	Collections / Expenditures	Encumbrances	Available Budget
Revenue									
Public Works									
30241100-371000	DONATION FROM PRIVATE SOURCE			\$ -	\$ 4,496	\$ 4,496	\$ 4,496		\$ 0
	subtotal			\$ -	\$ 4,496	\$ 4,496	\$ 4,496		\$ 0
Non-Departmental									
30290200-361000	INTEREST EARNINGS			\$ -	\$ -	\$ -	\$ 1,729		\$ (1,729)
30290200-362000	REALIZED GAIN/LOSS ON INVS			-	-	-			-
30290200-363000	UNREALIZED GAIN/LOSS INV			-	-	-	3,639		(3,639)
30290200-391100	TRANSFER IN/GENERAL FUND MATCH			4,200,000	-	4,200,000	350,000		3,850,000
30290200-395000	CARRYFORWARD FUND BALANCE			-	1,716,691	1,716,691	-		1,716,691
	subtotal			\$ 4,200,000	\$ 1,716,691	\$ 5,916,691	\$ 355,368		\$ 5,561,323
	Total			\$ 4,200,000	\$ 1,721,187	\$ 5,921,187	\$ 359,863		\$ 5,561,324
Expenditures									
Public Works									
30241100-541430 C1216	SW DRAINAGE MAINTENANCE	1,006,297	629,804	\$ 150,000	\$ 226,493	\$ 376,493	\$ 6,691	\$ 11,391	\$ 358,411
30241100-541430 C1308	SW PIPE & STRUCTURE R&M	11,429,215	6,438,340	3,930,000	1,060,875	4,990,875	20,492	790,707	4,179,677
30241100-541430 C1503	STORMWATER STUDIES	500,001	323,580	-	176,421	176,421	-	20,200	156,221
30241100-541430 C1604	STORMWATER INSPECTIONS	664,054	458,719	120,000	85,335	205,335	-	83,645	121,690
30241100-541430 C2208	MEADOW BROOK HILLS DRAINAGE	250,000	150,800	-	99,200	99,200	1,650	81,200	16,350
30261150-541430 C1919	WILLS PARK STREAM RESTORATION	7,214	7,214	-	-	-	-	-	-
	subtotal			\$ 4,200,000	\$ 1,648,324	\$ 5,848,324	\$ 28,833	\$ 987,142	\$ 4,832,349
Non-Departmental									
30290200-579000	NON-ALLOCATED			\$ -	\$ 72,863	\$ 72,863	\$ -	\$ -	\$ 72,863
	subtotal			\$ -	\$ 72,863	\$ 72,863	\$ -	\$ -	\$ 72,863
	Total			\$ 4,200,000	\$ 1,721,187	\$ 5,921,187	\$ 28,833	\$ 987,142	\$ 4,905,212



CITY OF ALPHARETTA
 Financial Management Reports
 Capital Project Funds
American Rescue Act Fund Detail (Fund 303; life-to-date for all projects)
 As of July 31, 2022

		Project Snapshot: FY2017 - FY2022		FY 2023					
Account #	Project	Total Project Authorization	Prior Year Actuals	Original Appropriation	Transfers / Adjustments	Revised Budget	Collections / Expenditures	Encumbrances	Available Budget
Revenue									
General Government									
30390200-331350	FEDERAL GRANT	-	6,644,511	\$	-	\$	-	\$	-
30390200-395000	CARRYFORWARD FUND BALANCE				-	4,199,000	4,199,000	-	4,199,000
	Total			\$	-	\$ 4,199,000	\$ 4,199,000	\$ -	\$ 4,199,000
Expenditures									
Public Works									
30341100-541410 C1219	MILLING & RESURFACING	1,176,000	1,175,955	\$	-	\$ 45	\$ 45	\$ -	\$ 45
30341100-541430 C1308	PIPE/STORM STRUCTURE REPLACEMENT	2,144,510	939,002		-	1,205,508	1,205,508	823	1,196,103
30341100-541420 C1801	SIDEWALK MAINTENANCE/REPAIR	1,324,001	269,139		-	1,054,862	1,054,862	1,376	258,605
	subtotal			\$	-	\$ 2,260,415	\$ 2,260,415	\$ 2,199	\$ 1,454,753
Recreation, Parks & Cultural Services									
30361150-541500 C1636	GREENWAY REPAIR/MAINTENANCE	2,000,000.00	61,415	\$	-	\$ 1,938,585	\$ 1,938,585	\$ -	\$ 24,996
	subtotal			\$	-	\$ 1,938,585	\$ 1,938,585	\$ -	\$ 24,996
	Total			\$	-	\$ 4,199,000	\$ 4,199,000	\$ 2,199	\$ 1,479,749
				\$	-	\$ 4,199,000	\$ 4,199,000	\$ 2,199	\$ 1,479,749
				\$	-	\$ 4,199,000	\$ 4,199,000	\$ 2,199	\$ 1,479,749
				\$	-	\$ 4,199,000	\$ 4,199,000	\$ 2,199	\$ 1,479,749



CITY OF ALPHARETTA

Financial Management Reports

Capital Project Funds

2016 Parks and Transportation Bond Fund Detail (Fund 317; life-to-date for all projects)

As of July 31, 2022

			Project Snapshot: FY2017 - FY2022		FY 2023					
			Total Project Authorization	Prior Year Actuals	Original Appropriation	Transfers / Adjustments	Revised Budget	Collections / Expenditures	Encumbrances	Available Budget
Account #	Project									
Revenue										
Non-Departmental										
31790200-395000	CARRYFORWARD FUND BALANCE				\$ -	\$ 190,370	\$ 190,370	\$ -		\$ 190,370
31790200-389000	MISCELLANEOUS REVENUE				-	108,000	108,000	-		108,000
31790200-361000	INTEREST EARNINGS				-	-	-	1,931		(1,931)
	subtotal				\$ -	\$ 298,370	\$ 298,370	\$ 1,931		\$ 296,439
	Total				\$ -	\$ 298,370	\$ 298,370	\$ 1,931		\$ 296,439
Expenditures										
31741100-541410	C1410	RUCKER RD CORRIDOR	14,651,644	14,651,644	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -
31741100-541410	C1631	MCGINNIS RD IGA (FORSYTH)	3,773,587	3,773,587	-	-	-	-	-	-
31741100-541410	C1702	KIMBALL BR RD IMPROVEMENTS	9,872,926	9,872,926	-	-	-	-	-	-
31741100-541420	C1712	ALPHALOOP	449,253	359,043	-	90,210	90,210	-	90,210	0
31741100-541420	C1715	BETHANY/MAYFIELD ROUNDABOUT	299,137	299,137	-	-	-	-	-	-
31741100-541420	C1826	SPRUELL CIRCLE SIDEWALK	233,319	232,819	-	500	500	-	499	1
31741100-541420	C1829	PROVIDENCE AREA SIDEWALKS	920,441	920,441	-	-	-	-	-	-
31741100-541420	C1925	MORRISON PARKWAY SIDEWALKS	921,718	921,718	-	-	-	-	-	-
31741100-541420	C2305	ALPHALOOP (OMP - NORTHWINDS)	50,749	-	-	50,749	50,749	-	-	50,749
31761150-541300	C1708	GREENWAY EXT TO FORSYTH	9,842,189	9,837,210	-	4,979	4,979	-	-	4,979
31761150-541300	C1709	EASTSIDE COMMUNITY CTR	2,553,436	2,519,186	-	34,250	34,250	-	34,250	-
31741100-579000	PW RESERVE		-	-	-	-	-	-	-	-
31761150-579000	PARKS RESERVE		117,682	-	-	117,682	117,682	-	-	117,682
	Total				\$ -	\$ 298,370	\$ 298,370	\$ -	\$ 124,959	\$ 173,411



CITY OF ALPHARETTA
 Financial Management Reports
 Capital Project Funds
2022 Parks Bond Fund Detail (Fund 318; life-to-date for all projects)
 As of July 31, 2022

			Project Snapshot: FY2017 - FY2022		FY 2023					
			Total Project Authorization	Prior Year Actuals	Original Appropriation	Transfers / Adjustments	Revised Budget	Collections / Expenditures	Encumbrances	Available Budget
Account #	Project									
Revenue										
Non-Departmental										
31890200-361000	INTEREST EARNINGS				\$ -	\$ -	\$ -	\$ 38,780		\$ (38,780)
3180200-393310	BOND PROCEEDS				-	-	-	-		-
31890200-393400	BOND PREMIUM					28,908,660	28,908,660	-		28,908,660
31890200-395000	CARRYFORWARD FUND BALANCE				-	367,339	367,339	-		367,339
	subtotal				\$ -	\$ 29,275,999	\$ 29,275,999	\$ 38,780		\$ 29,237,219
	Total				\$ -	\$ 29,275,999	\$ 29,275,999	\$ 38,780		\$ 29,237,219
Expenditures										
31841100-541420	C1712	ALPHALOOP	7,500,000	-	\$ -	\$ 7,500,000	\$ 7,500,000	\$ -	\$ -	\$ 7,500,000
31861150-541500	C0922	SYNTHETIC TURF	1,000,000	23,990	-	976,010	976,010	-	-	976,010
31861150-541500	C1911	EQUESTRIAN CENTER (CITY)	5,000,000	11,664	-	4,988,336	4,988,336	-	31,524	4,956,812
31861150-541500	C2011	WILLS PARK MASTER PLAN IMP	5,671,367	125,098	-	5,546,269	5,546,269	-	27,215	5,519,054
31861150-541500	C2216	UNION HILL PARK	3,250,001	25,753	-	3,224,248	3,224,248	-	-	3,224,248
31861150-541500	C2217	MID-BROADWELL PARK	500,001	47,538	-	452,463	452,463	-	2,475	449,988
31861150-541500	C2218	OLD RUCKER PARK	3,000,000	20,170	-	2,979,830	2,979,830	-	-	2,979,830
31861150-541500	C2219	FARMHOUSE PARK	2,000,000	16,720	-	1,983,280	1,983,280	-	-	1,983,280
31861150-541500	C2220	WATERS ROAD PARK	1,250,000	15,126	-	1,234,874	1,234,874	-	779	1,234,095
31861150-541500	C2245	WILLS PARK MAINTENANCE FACIL	328,634	-	-	328,634	328,634	-	328,634	-
31890200-579000	PARKS RESERVE		62,055	-	-	62,055	62,055	-	-	62,055
31890200-584000	DEBT ISSUANCE COSTS		368,549	368,549	-	-	-	-	-	-
	Total				\$ -	\$ 29,275,999	\$ 29,275,999	\$ -	\$ 390,626	\$ 28,885,373



CITY OF ALPHARETTA
 Financial Management Reports
 Capital Project Funds
TSPLOST Fund Detail (Fund 335; life-to-date for all projects)
 As of July 31, 2022

Account #Project		Project Snapshot: FY2017 - FY2022		FY 2023					Available Budget
		Total Project Authorization	Prior Year Actuals	Original Appropriation	Transfers / Adjustments	Revised Budget	Collections / Expenditures	Encumbrances	
Revenue									
Non-Departmental									
33590200-395000	CARRYFORWARD FUND BALANCE			\$ 4,300,000	\$ 37,247,282	\$ 41,547,282			\$ 41,547,282
33590200-313400	TSPLOST			-	-	-			-
33541100-361000	INTEREST EARNINGS			-	-	-	58,954		(58,954)
	Total			\$ 4,300,000	\$ 37,247,282	\$ 41,547,282	\$ 58,954		\$ 41,488,328
Expenditures									
33541100-541410	ROADWAY IMPROVEMENTS	121,934	121,934	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -
33541100-541410	C1219 MILLING AND RESURFACING	2,000,000	-	2,000,000	-	2,000,000	-	-	2,000,000
33541100-541410	C1631 MCGINNIS RD IGA (FORSYTH)	5,026,414	184,456	-	4,841,958	4,841,958	24,500	-	4,817,458
33541100-541410	C1713 KIMBALL BR RD OP IMPROVEMENTS	1,359,742	1,119,002	-	240,740	240,740	-	233,749	6,991
	BETHANY RD @ MID BROADWELL								
33541100-541410	C1714 RD	1,174,001	1,174,001	-	-	-	-	-	-
33541100-541410	C1715 BETHANY RD @ MAYFIELD RD	1,648,759	1,648,759	-	-	-	-	-	-
33541100-541410	C1717 OLD MILTON PKWY CAPACITY IMP	5,579,474	1,924,663	-	3,654,811	3,654,811	-	1,654,810	2,000,001
33541100-541410	C1800 HAYNES BRIDGE RD IMP	197,826	187,598	-	10,228	10,228	-	10,228	0
33541100-541410	C1932 ACADEMY ST IMPROVEMENTS	275,490	275,490	-	-	-	-	-	-
	WEBB BRIDGE RD (DESIGN-PROJ. MGMT., ETC.)								
33541100-541410	C1933	876,389	860,986	-	15,403	15,403	-	15,403	1
	WINDWARD PKWY EAST IMPROVEMENTS								
33541100-541410	C1934	1,614,835	1,263,692	-	351,143	351,143	-	351,143	-
	WINDWARD PKWY WEST IMPROVEMENTS								
33541100-541410	C1935	985,508	985,508	-	-	-	-	-	-
33541100-541410	C2054 GA 400 BRIDGES (WEBB; KIMBALL)	4,886,001	737,429	-	4,148,572	4,148,572	-	4,148,571	1
	WEBB BR RD PHASE 4 (NPP TO GREENWAY)								
33541100-541410	C2104	692,509	676,585	-	15,924	15,924	-	15,923	1
33541100-541410	C2113 ENCORE GREENWAY GATEWAY	2,573,000	230,000	2,300,000	43,000	2,343,000	-	43,000	2,300,000
	WEBB BRIDGE RD PHASE 1 (WESTWIND TO GREENWAY)								
33541100-541410	C2211	874,801	725,037	-	149,764	149,764	-	149,763	1
	WEBB BRIDGE RD PHASE 2 (ROUNDABOUT-PARK)								
33541100-541410	C2229	6,000,000	54,157	-	5,945,843	5,945,843	-	3,982	5,941,862
	WEBB BRIDGE RD PHASE 3 (GREENWAY-ROUNDABOUT)								
33541100-541410	C2232	17,000,000	33,550	-	16,966,450	16,966,450	18,887	-	16,947,563
	GREENWAY EXTENSION TO FORSYTH								
33561150-541300	C1708	1,000,000	1,000,000	-	-	-	-	-	-
33590200-579000	CONTINGENCY			-	863,446	863,446	-	-	863,446
	Total			\$ 4,300,000	\$ 37,247,282	\$ 41,547,282	\$ 43,387	\$ 6,626,571	\$ 34,877,324



CITY OF ALPHARETTA
 Financial Management Reports
 Capital Project Funds
TSPLOST 2 Fund Detail (Fund 336; life-to-date for all projects)
 As of July 31, 2022

				Project Snapshot: FY2017 - FY2022		FY 2023					
				Total Project Authorization	Prior Year Actuals	Original Appropriation	Transfers / Adjustments	Revised Budget	Collections / Expenditures	Encumbrances	Available Budget
Account #	Project										
Revenue											
Non-Departmental											
33690200-313400	TSPLOST 2					\$ -	\$ 49,586,538	\$ 49,586,538	\$ 1,250,006		\$ 48,336,532
33690200-395000	CARRYFORWARD FUND BALANCE					-	2,397,197	2,397,197	-		2,397,197
Total						\$ -	\$ 51,983,735	\$ 51,983,735	\$ 1,250,006		\$ 50,733,729
Expenditures											
33641100-541410	C2040	TRADEWINDS PARKWAY		6,500,000	2,400	\$ -	\$ 6,497,600	\$ 6,497,600	\$ 1,265	\$ -	\$ 6,496,335
33641100-541410	C2104	WEBB BRIDGE ROAD (NPP-GREENWAY)		13,000,000	13,873	-	12,986,127	12,986,127	-	23,450	12,962,677
33641100-541410	C2107	NORTH POINT PARKWAY IMP		10,000,000	-	-	10,000,000	10,000,000	-	-	10,000,000
33641100-541410	C2221	CROSSWALK (ALPHARETTA ELEM)		113,037	18,537	-	94,500	94,500	-	94,500	-
33641100-541410	C2222	CROSSWALK (MANNING OAKS ELEM)		74,263	18,537	-	55,726	55,726	-	-	55,726
33641100-541410	C2223	CROSSING (92 MILTON GARAGE)		212,300	-	-	212,300	212,300	-	212,300	-
33641100-541410	C2224	RAISED INTSECTION (MARIETTA ST)		350,001	1,525	-	348,476	348,476	-	14,675	333,801
33641100-541410	C2225	CROSSINGS (CITY CTR/CHURCHES)		750,000	1,161	-	748,839	748,839	-	15,039	733,800
33641100-541410	C2226	PEDESTRIAN BRIDGES (WW PKWY)		4,000,000	12,349	-	3,987,651	3,987,651	-	180,701	3,806,950
33641100-541410	C2227	CROSSWALK (COGBURN PARK)		149,401	-	-	149,401	149,401	-	149,401	0
33641100-541410	C2228	CROSWALK (CHARLOTTE DR)		146,000	-	-	146,000	146,000	-	146,000	-
33641100-541410	C2230	CUMMING ST CORRIDOR		4,757,526	-	-	4,757,526	4,757,526	-	-	4,757,526
33641100-541420	C2305	ALPHALOOP (OMP - NORTHWINDS)		12,000,000	411	-	11,999,589	11,999,589	5,400	-	11,994,189
Total						\$ -	\$ 51,983,735	\$ 51,983,735	\$ 6,665	\$ 836,066	\$ 51,141,004



CITY OF ALPHARETTA
 Financial Management Reports
 Special Revenue Funds
Impact Fee Fund (Fund 270; life-to-date for active projects)
 As of July 31, 2022

				Project Snapshot: FY2013 - FY2022		FY 2023					
				Total Project Authorization	Prior Year Actuals	Original Appropriation	Transfers / Adjustments	Revised Budget	Collections / Expenditures	Encumbrances	Available Budget
Account #	Project										
Revenue											
27074110-341321	IMPACT FEES STREETS & HIGHWAYS					\$ -	\$ -	\$ -	\$ 5,083		\$ (5,083)
27074110-341323	IMPACT FEES RECREATION & PARKS					350,000	34,089	384,089	15,418		368,671
27074110-341324	IMPACT FEES PUBLIC SAFETY					-	-	-	774		(774)
27074110-395000	CARRYFORWARD FUND BALANCE					1,668,690	3,234,586	4,903,276			4,903,276
27074110-362000	REALIZED GAIN/LOSS ON INVS					-	-	-			-
27074110-363000	UNREALIZED GAIN/LOSS					-	-	-	9,221		(9,221)
27074110-361000	INTEREST EARNINGS					-	-	-	4,381		(4,381)
	Total					\$ 2,018,690	\$ 3,268,675	\$ 5,287,365	\$ 34,878		\$ 5,252,487
Expenditures											
Public Safety											
27031150-544200	C2206	RAPID RESCUE TRUCK		124,600	124,100	\$ -	\$ 500	\$ 500	\$ -		\$ 500
27031150-542100	C2302	ALL TERRAIN VEHICLES		18,690	-	18,690	-	18,690	-		18,690
	subtotal					\$ 18,690	\$ 500	\$ 19,190	\$ -	\$ -	\$ 19,190
Public Works											
27041100-541410	C1410	RUCKER RD CORRIDOR		1,002,553	857,003	\$ -	\$ 145,550	145,550	\$ 145,550		\$ 0
27041100-541410	C1723	TEASLEY ST IMPROVEMENTS		56,925	38,125	-	18,800	18,800	-		18,800
27041100-541410	C2107	NORTH POINT PARKWAY IMPROVEMENTS		1,250,000	-	-	1,250,000	1,250,000	-		1,250,000
27041100-541420	C2305	ALPHALOOP (OMP - NORTHWINDS)		500,000	-	-	500,000	500,000	19,000		481,000
	subtotal					\$ -	\$ 1,914,350	\$ 1,914,350	\$ -	\$ 164,550	\$ 1,749,800
Recreation, Parks & Cultural Services											
27061150-541500	C2011	WILLS PARK MASTER PLAN		328,634	-	\$ -	\$ 328,634	\$ 328,634	\$ -		\$ 328,634
27061150-541410	C2113	ENCORE GREENWAY GATEWAY		2,000,000	-	2,000,000	-	2,000,000	-		2,000,000
	subtotal					\$ 2,000,000	\$ 328,634	\$ 2,328,634	\$ -	\$ -	\$ 2,328,634



CITY OF ALPHARETTA
 Financial Management Reports
 Special Revenue Funds
Impact Fee Fund (Fund 270; life-to-date for active projects)
 As of July 31, 2022

Account #	Project	Project Snapshot: FY2013 - FY2022		FY 2023					Available Budget
		Total Project Authorization	Prior Year Actuals	Original Appropriation	Transfers / Adjustments	Revised Budget	Collections / Expenditures	Encumbrances	
Non-Departmental									
27074110-521200	PROFESSIONAL SERVICES			\$ -	\$ 66,720	\$ 66,720		\$ 66,720	\$ -
27074110-579001	NON-ALLOCATED STREETS & HIGHWAYS			-	841,016	841,016	-	-	841,016
27074110-579002	NON-ALLOCATED RECREATION & PARKS			-	-	-	-	-	-
27074110-579003	NON-ALLOCATED PUBLIC SAFETY			-	117,455	117,455	-	-	117,455
27041100-579011	MATCH (GRANTS UNDER REVIEW)			-	-	-	-	-	-
	subtotal			\$ -	\$ 1,025,191	\$ 1,025,191	\$ -	\$ 66,720	\$ 958,471
	Total			\$ 2,018,690	\$ 3,268,675	\$ 5,287,365	\$ -	\$ 231,270	\$ 5,056,095



CITY OF ALPHARETTA
 Financial Management Reports
 Special Revenue Funds
Hotel/Motel Fund (Fund 275; life-to-date for active projects)
 As of July 31, 2022

		Project Snapshot: FY2013 - FY2022		FY 2023					
Account #	Project	Total Project Authorization	Prior Year Actuals	Original Appropriation	Transfers / Adjustments	Revised Budget	Collections / Expenditures	Encumbrances	Available Budget
Revenue									
27590150-314100	HOTEL/MOTEL TAXES			\$ 7,500,000	\$ -	\$ 7,500,000	\$ 888,307		\$ 6,611,693
27590150-319201	PENALTY/INTEREST HOTEL/MOTEL TAXES			-	-	-			-
27590150-362000	REALIZED GAIN/LOSS ON INVS			-	-	-			-
27590150-363000	UNREALIZED GAIN/LOSS			-	-	-	2,724		(2,724)
27590150-361000	INTEREST EARNINGS			-	-	-	1,294		(1,294)
	subtotal			\$ 7,500,000	\$ -	\$ 7,500,000	\$ 892,324		\$ 6,607,676
Non-Departmental									
27590150-395000	CARRYFORWARD FUND BALANCE		-	\$ -	\$ 974,971	\$ 974,971	\$ -		\$ 974,971
	subtotal			\$ -	\$ 974,971	\$ 974,971	\$ -		\$ 974,971
	Total			\$ 7,500,000	\$ 974,971	\$ 8,474,971	\$ 892,324		\$ 7,582,647
Expenditures									
Alpharetta Convention & Visitors Bureau									
27590150-572002	ALPHA CONV & VISITORS BUREAU DISTRIBUTION	29,555,268	26,274,018	\$ 3,281,250	\$ -	\$ 3,281,250	\$ -		\$ 3,281,250
	subtotal			\$ 3,281,250	\$ -	\$ 3,281,250	\$ -		\$ 3,281,250
City/Other									
27590150-521200	PROFESSIONAL SERVICES	35,655	30,155	\$ 5,500	\$ -	\$ 5,500	\$ 2,915	\$ -	\$ 2,585
27590150-579006	DEBT SERVICE RESERVE	417,821	-	35,537	382,284	417,821		-	417,821
27590150-611100	CITY OF ALPHARETTA DISTRIBUTION	25,731,799	22,919,299	2,812,500	-	2,812,500	333,115	-	2,479,385
	subtotal			\$ 2,853,537	\$ 382,284	\$ 3,235,821	\$ 336,030	\$ -	\$ 2,899,791
Tourism Product Development									
27590150-541500	C1911 EQUESTRIAN CENTER	38,739	38,739	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -
27590450-541500	C2011 WILLS PARK MASTER PLAN	751,891	468,574	-	283,317	283,317		276,047	7,270
27590150-541500	C2245 WILLS PRK MAINTENANCE FACILITY	309,370	-	-	309,370	309,370		309,369	1
27590151-581100	D1600 PRINCIPAL (2016 CONF CTR BOND)	2,185,000	1,535,000	650,000	-	650,000		-	650,000
27590151-582100	D1600 INTEREST PAYMENT (2016 CONF CTR BOND)	5,343,655	4,628,442	715,213	-	715,213		-	715,213
	subtotal			\$ 1,365,213	\$ 592,687	\$ 1,957,900	\$ -	\$ 585,417	\$ 1,372,483
	Total			\$ 7,500,000	\$ 974,971	\$ 8,474,971	\$ 336,030	\$ 585,417	\$ 7,553,524



OTHER REPORTS



CITY OF ALPHARETTA
Financial Management Reports
Listing of Payments \$5,000 and greater
for the month ended July 31, 2022

Vendor	Description	Department	\$ Amount
A. B. GYMNASTICS LLC	AGA CLASSES	Rec., Parks & Cultural Services	\$ 13,443.37
ALLIED WASTE SERVICE	WASTE MANAGEMENT SERVICES	Finance	\$ 6,316.28
AMT FLEET SERVICES	TRUCK MAINTENANCE AND REPAIR, HEAVY	Rec., Parks & Cultural Services	\$ 6,937.41
ANDREWS TECHNOLOGY	TIME AND ATTENDANCE DATA COLLECTION SYSTEMS	Various Departments	\$ 45,669.00
AT&T/BELLSOUTH @ 85	TELEPHONE SERVICES, LONG DISTANCE AND LOCAL	Public Safety	\$ 5,726.28
AT&T/BELLSOUTH @ 85	TELEPHONE SERVICES, LONG DISTANCE AND LOCAL	Public Safety	\$ 17,431.77
BIDDLE CONSULTING	SOFTWARE MAINTENANCE/SUPPORT - EXP DATE 07/05/23	Public Safety	\$ 5,495.00
BONFIRE INTERACTIVE	SOFTWARE MAINTENANCE/SUPPORT	Finance	\$ 24,833.69
BUTCH THOMPSON	CONSTRUCTION, SEWER AND STORM DRAIN	Public Works	\$ 20,492.00
CALLOWAY TITLE	TITLE REPORT FOR ROW ACQUISITION	Public Works	\$ 17,820.00
CAMBRIDGE INVESTMENT	CONSULTING FEE	Finance	\$ 8,381.01
CBK MECHANICAL INC	ENCAPSULANT, TRAFFIC LOOP DETECTOR	Public Works	\$ 8,100.00
CITY OF MILTON	LEASE-COURTROOM IGA-JULY 2022	Municipal Court	\$ 6,775.00
CIVICPLUS	SOFTWARE MAINTENANCE/SUPPORT	City Clerk	\$ 15,021.34
CIVICPLUS	SOFTWARE MAINTENANCE/SUPPORT	Various Departments	\$ 9,942.35
CLEARVIEW AI INC	SOFTWARE MAINTENANCE/SUPPORT	Public Safety	\$ 5,500.00
COMMISSION ON ACCREDITATION (CALEA)	ACCREDITATION FEES	Public Safety	\$ 7,855.00
CORPORATE HEALTH	HEALTH CARE SERVICES (NOT OTHERWISE CLASSIFIED)	Finance	\$ 56,131.35
CRABAPPLE TURF	GROUNDS REPAIR & MAINTENANCE	Rec., Parks & Cultural Services	\$ 10,046.13
ECHELON FRONT LLC	INSTRUCTOR-LED, CLASSROOM TRAINING (NON-TECHNICAL)	Public Safety	\$ 13,000.00
EPL HOLDINGS, LLC	ALPHALOOP (OMP-NORTHWINDS)	Public Works	\$ 5,400.00
ESIS INC	RIMS SERVICES, WORKERS COMP	Risk Management	\$ 8,500.00
ESRI	ESRI SOFTWARE-GEOGRAPHIC INFORMATION SYSTEM (GIS)	Various Departments	\$ 60,500.00
FIVE OAKS FENCE COMPANY	FENCING, ORNAMENTAL	Rec., Parks & Cultural Services	\$ 20,444.00
GALLS INC	EMPLOYEE UNIFORMS	Public Safety	\$ 6,748.65



CITY OF ALPHARETTA
 Financial Management Reports
Listing of Payments \$5,000 and greater
 for the month ended July 31, 2022

Vendor	Description	Department	\$ Amount
GREENTREE SHAVINGS	BEDDING (ALL TYPES)	Rec., Parks & Cultural Services	\$ 5,430.60
GREG MALCOLM & ASSOCIATES	APPRAISAL FEE; MCGINNIS RD IGA (FORSYTH)	Public Works	\$ 24,500.00
HARDY CHEVROLET INC	CLASS 1 TRUCKS (6,000 LB. GVWR OR LESS)	Public Works	\$ 42,975.00
HOME BY DARK PRODUCT	AMUSEMENT AND ENTERTAINMENT SERVICES	Rec., Parks & Cultural Services	\$ 30,000.00
INNOVATIVE DATA	COMPUTER SOFTWARE CONSULTING	Public Safety	\$ 8,352.55
LD GYMNASTICS INC	INSTRUCTORS, CLASSES FOR THE PUBLIC	Rec., Parks & Cultural Services	\$ 15,016.07
NORTH FULTON REGIONAL RADIO SYS. AUTH.	RADIO FREQUENCY ACCESS SERVICES	Various Departments	\$ 166,488.35
OPENGOV INC	SOFTWARE MAINTENANCE/SUPPORT	Finance	\$ 12,000.00
PLAY WELL TEKNOLOGIE	INSTRUCTORS, CLASSES FOR THE PUBLIC	Rec., Parks & Cultural Services	\$ 5,880.00
POPCORN MEDIA LLC	INSTRUCTORS, CLASSES FOR THE PUBLIC	Rec., Parks & Cultural Services	\$ 9,697.50
PRAETORIAN DIGITAL	TRAINING, COMPUTER BASED (SOFTWARE SUPPORTED)	Public Safety	\$ 7,245.00
PYRO SHOWS EAST COAST INC	FIREWORKS DISPLAY AND CARNIVAL SERVICES	Rec., Parks & Cultural Services	\$ 17,500.00
RELIABLE TRAFFIC	TRAFFIC COUNTING SERVICES	Public Works	\$ 8,140.00
RHYTHM N SHOES LLC	INSTRUCTORS, CLASSES FOR THE PUBLIC	Rec., Parks & Cultural Services	\$ 7,029.00
RHYTHM N SHOES LLC	INSTRUCTORS, CLASSES FOR THE PUBLIC	Rec., Parks & Cultural Services	\$ 7,635.38
SAVATREE LLC	TREE AND SHRUB REMOVAL SERVICES	Rec., Parks & Cultural Services	\$ 7,905.00
SAVATREE LLC	TREE AND SHRUB REMOVAL SERVICES	Rec., Parks & Cultural Services	\$ 13,175.00
SAVILLE & COMPANY	FY2023 INSURANCE PREMIUM RENEWAL	Risk Management	\$ 628,796.00
SAWNEE ELECTRIC MEMBERSHIP CORP	ELECTRICITY UTILITIES	Various Departments	\$ 13,008.34
SPRINTURF	Contract Withholding: 21-108 RETAINAGE RELEASE	General Government	\$ 8,225.00
TECH ALPHARETTA	ATC OPERATIONAL FUNDS	Development Authority	\$ 7,916.67
TECH ALPHARETTA	ATC OPERATIONAL FUNDS	Development Authority	\$ 7,916.67
TRANSCEND ROBOTICS	POLICE INVESTIGATION ROBOTS	Public Safety	\$ 16,500.00
TYLER TECHNOLOGIES	SOFTWARE MAINTENANCE/SUPPORT	Finance	\$ 9,543.98
USI INSURANCE	CYBER LIABILITY POLICY FY23	Risk Management	\$ 78,156.00
USI INSURANCE	WORKER'S COMP EXCESS LIABILITY	Risk Management	\$ 155,831.00
USI INSURANCE	COMMERCIAL LINES SERVICE FEE FY2023	Risk Management	\$ 50,000.00
VERIZON WIRELESS SERVICES LLC	TELEPHONE SERVICES, CELLULAR	Various Departments	\$ 6,139.13



CITY OF ALPHARETTA
Financial Management Reports
Listing of PO's between \$5,000.01 and \$50,000.00
for the month ended July 31, 2022

Purchase Order #	Vendor	Department	Purchase Order Amt.	Description
23000001	BONFIRE INTERACTIVE	FINANCE	\$ 24,833.69	PROCUREMENT AND CONTRACT SOFTWARE RENEWAL
23000007	OPENGOV, INC	FINANCE	\$ 12,000.00	OPENGOV FINANCIAL INTEGRATION AND MANAGEMENT REPORTING SOFTWARE RENEWAL
23000008	8A TRANSLATIONS	MUNICIPAL COURT	\$ 35,000.00	FY23 TRANSLATION SERVICES
23000010	COMFORT BY DESIGN INC	PUBLIC WORKS	\$ 32,962.00	FY23 HEATING/AIR CONDITIONAL MAINTENANCE
23000011	WATT COMMERCIAL SWEEPING	PUBLIC WORKS	\$ 7,920.00	FY23 STREET SWEEPING SERVICES FOR PARKING DECKS
23000013	CAPITAL CITY ELECTRICAL SERVICES, LLC	PUBLIC WORKS	\$ 6,931.20	FY23 MONTHLY STREETLIGHT AND PEDESTRIAN LIGHT MAINTENANCE INSPECTIONS
23000015	TYLER TECHNOLOGIES INC	FINANCE	\$ 9,543.98	SOCRATA SOFTWARE RENEWAL
23000016	BUILDING MANAGEMENT CONSULTANTS, LLC	PUBLIC WORKS	\$ 12,000.00	FLAT ROOF PREVENTATIVE MAINTENANCE AT MULTIPLE LOCATIONS
23000017	THYSSENKRUPP ELEVATOR CORP	PUBLIC WORKS	\$ 10,548.00	FY23 CITY HALL PARKING DECK AND MILTON AVE PARKING DECK ELEVATOR MAINTENANCE
23000018	ARROW EXTERMINATORS	PUBLIC WORKS	\$ 12,924.00	FY23 MONTHLY PEST CONTROL AT CITY FACILITIES
23000019	POWER & ENERGY SERVICES INC	PUBLIC WORKS	\$ 22,952.00	FY23 MONTHLY GENERATOR INSPECTIONS AT MULTIPLE FACILITEIS
23000022	WATT COMMERCIAL SWEEPING	PUBLIC WORKS	\$ 30,819.50	FY23 STREET SWEEPING SERVICES
23000028	ONE SOURCE COUNSELING AND EMPLOYEE	FINANCE	\$ 15,360.00	FY23 EMPLOYEE ASSISTANCE PROGRAM
23000031	MEER ELECTRICAL CONTRACTORS INC	PUBLIC WORKS	\$ 12,540.00	FY23 TORNADO SIREN MAINTENANCE
23000032	COMCAST OF GEORGIA INC	INFORMATION TECHNOLOGY	\$ 18,000.00	FY23 ETHERNET DEDICATED INTERNET
23000039	INNOVATIVE DATA SOLUTIONS	PUBLIC SAFETY	\$ 8,352.55	POWER DMS LICENSE RENEWAL
23000042	BREWICK ENTERPRISES LLC	COMMUNITY DEVELOPMENT	\$ 8,880.00	INSTALLATION OF CERAMIC TILE AT TECH ALPHARETTA RESTROOMS
23000043	BREWICK ENTERPRISES LLC	COMMUNITY DEVELOPMENT	\$ 5,240.00	INSTALLATION OF CERAMIC TILE AT TECH ALPHARETTA RESTROOMS
23000044	CASE SYSTEMS INC	RECREATION, PARKS & CULTURAL SERVICES	\$ 38,360.55	UPGRADE (23) EXISTING CALL BOXES TO 4G
23000045	KINGS RIVER CASTING INC	RECREATION, PARKS & CULTURAL SERVICES	\$ 8,372.00	(6) SQUARE IRON VALLEY TRASH RECEPTACLES WITH 32-GALLON LINER
23000046	FIVE OAKS FENCE COMPANY INC	RECREATION, PARKS & CULTURAL SERVICES	\$ 17,420.00	REMOVAL OF EXISTING FENCE AND REPLACEMENT WITH 5' STEEL FENCE AT (2) PARKS
23000047	ROSITA CZEKALA	RECREATION, PARKS & CULTURAL SERVICES	\$ 8,802.50	FY23 INSTRUCTOR SERVICES - CLAY/POTTERY
23000049	POPCORN MEDIA LLC	RECREATION, PARKS & CULTURAL SERVICES	\$ 9,697.50	FY23 INSTRUCTOR SERVICES - MOVIE STAR CAMP
23000051	ELIZABETH DUNKIN	RECREATION, PARKS & CULTURAL SERVICES	\$ 6,900.00	FY23 INSTRUCTOR SERVICES - CAMP CREATIVE AND FLOWER ARRANGING
23000054	ICON ENTERPRISES, INC.	ADMINISTRATION	\$ 15,021.34	CIVIC CLERK AGENDA MANAGEMENT SOFTWARE RENEWAL
23000055	GRM INFORMATION MANAGEMENT SERVICES	FINANCE	\$ 30,670.00	RECORDING STORAGE AND SHREDDING SERVICES
23000060	AMT FLEET SERVICES INC	RECREATION, PARKS & CULTURAL SERVICES	\$ 6,937.41	TRANSMISSION, PTO, AND WATER PUMP REPAIRS ON EQUESTRIAN CENTER WATER TRUCK
23000064	ICON ENTERPRISES, INC.	PUBLIC WORKS	\$ 9,942.35	CIVIC PLUS SOFTWARE RENEWAL
23000068	FASHION WORKSHOPS LLC	RECREATION, PARKS & CULTURAL SERVICES	\$ 6,500.00	FY23 INSTRUCTOR SERVICES - FASHION DESIGN AND SEWING
23000069	CRABAPPLE TURF MANAGEMENT INC	RECREATION, PARKS & CULTURAL SERVICES	\$ 23,287.55	CONSTRUCT (3) DRY STACK STONE TIERED SEATING WALLS AT EQUESTRIAN CENTER
23000070	PYRO SHOWS EAST COAST INC	RECREATION, PARKS & CULTURAL SERVICES	\$ 17,500.00	FINAL PAYMENT FOR JULY 4TH FIREWORK DISPLAY
23000074	UTILITIES PROTECTION CENTER INC	PUBLIC WORKS	\$ 5,522.51	FY23 UTILITIES PROTECTION MEMBERSHIP
23000075	NATIONAL OFFICE FURNITURE, INC	HUMAN RESOURCES	\$ 6,235.26	FURNITURE FOR CITY HALL ROOM 208
23000078	BIDDLE CONSULTING GROUP INC	PUBLIC SAFETY	\$ 5,495.00	TESTGENIUS CRITICAL ANNUAL SOFTWARE RENEWAL
23000080	ECHOLON FRONT LLC	PUBLIC SAFETY	\$ 13,000.00	REGISTRATION FOR (10) PUBLIC SAFETY EMPLOYEES TO ATTEND MUSTER 015 - TRAINING
23000081	DC POOL SERVICE LLC.	RECREATION, PARKS & CULTURAL SERVICES	\$ 35,100.00	FY23 CITY CENTER WATER FEATURES AND (4) OTHER FOUNTAINS MAINTENANCE
23000082	DC POOL SERVICE LLC.	RECREATION, PARKS & CULTURAL SERVICES	\$ 39,840.00	FY23 WILLS PARK POOL MAINTENANCE, POOL CHEMICALS, EMERGENCY CALLS
23000083	HIS MAJESTY COACHES INC	RECREATION, PARKS & CULTURAL SERVICES	\$ 10,368.00	BUS TRANSPORTATION FOR VARIOUS CAMPS
23000084	HOME BY DARK PRODUCTIONS LLC	RECREATION, PARKS & CULTURAL SERVICES	\$ 30,000.00	BROOKE STREET PARK CONCERT SERIES FOR JULY - SEPT 2022
23000085	MASON TRACTOR COMPANY INC	RECREATION, PARKS & CULTURAL SERVICES	\$ 15,071.10	(1) KUBOTA RTV-X900WL-H UTILITY VEHICLE
23000086	MISTRAL INC	PUBLIC SAFETY	\$ 5,130.00	(12) WOLFFTRACKER - THROUGH WALL SENSING DEVICES
23000087	BLUE LINE BREACHERS	PUBLIC SAFETY	\$ 5,970.00	(15) BANG BOX EXPLOSIVE MAGAZINES AND (3) BIG BANG BOX EXPLOSIVE MAGAZINE
23000088	BUTCH THOMPSON ENTERPRISES INC	PUBLIC WORKS	\$ 8,675.00	CURB AND GUTTER REPAIR WORK AT (3) LOCATIONS



CITY OF ALPHARETTA
Financial Management Reports
Listing of PO's between \$5,000.01 and \$50,000.00
for the month ended July 31, 2022

Purchase Order #	Vendor	Department	Purchase Order Amt.	Description
23000090	ZEST YOGA AND FITNESS	RECREATION, PARKS & CULTURAL SERVICES	\$ 8,640.00	FY23 INSTRUCTOR SERVICES - LINE DANCING
23000091	MARISSA SEQUEIRA	RECREATION, PARKS & CULTURAL SERVICES	\$ 8,640.00	FY23 INSTRUCTOR SERVICES - YOGA
23000093	MILO ENTERPRISES INC	PUBLIC WORKS	\$ 14,182.00	ADVANCE CONCRETE LIFTING AND LEVELING OF (90) TRIP HAZARDS ALONG MANSELL RD
23000096	AT&T	INFORMATION TECHNOLOGY	\$ 6,300.00	DSL LINES FOR GCIC CONNECTION FOR (2) DEPARTMENTS
23000101	YELLOWBEE STUDIO	RECREATION, PARKS & CULTURAL SERVICES	\$ 9,600.00	GRAPHIC DESIGN SERVICES FOR MONTHLY SEASONAL GUIDES
23000104	LAYER 3 COMMUNICATIONS, LLC	INFORMATION TECHNOLOGY	\$ 30,357.60	CORTEX XDR PRO ANTI-VIRUS/ANTI-MALWARE PROTECTION
23000106	PRAETORIAN GROUP INC	PUBLIC SAFETY	\$ 7,245.00	ANNUAL SUBSCRIPTION FOR ONLINE TRAINING CLASSES FOR FIRE AND EMS
23000108	BENNETT FIRE PRODUCTS CO INC	PUBLIC SAFETY	\$ 45,724.01	TURNOUT GEAR
23000110	RUTH AMIEL	RECREATION, PARKS & CULTURAL SERVICES	\$ 13,178.00	FY23 INSTRUCTOR SERVICES - PICKLEBALL
23000111	KARLA BLAGININ	RECREATION, PARKS & CULTURAL SERVICES	\$ 16,200.00	FY23 INSTRUCTOR SERVICES - PICKLEBALL
23000112	SPORTYKES	RECREATION, PARKS & CULTURAL SERVICES	\$ 21,000.00	FY23 INSTRUCTOR SERVICES - SPORTYKES FOR TODDLERS
23000115	NATIONAL OFFICE FURNITURE INC	RECREATION, PARKS & CULTURAL SERVICES	\$ 6,832.35	CONFERENCE TABLE AND CHAIRS
23000122	JIGNESH PANDYA	RECREATION, PARKS & CULTURAL SERVICES	\$ 9,959.88	FY23 INSTRUCTOR SERVICES - PICKLEBALL
23000124	ATL ENTERTAINMENT BASKETBALL LEAGUE	RECREATION, PARKS & CULTURAL SERVICES	\$ 35,000.00	FY23 INSTRUCTOR SERVICES - BASKETBALL
23000126	TIM BOWEN	RECREATION, PARKS & CULTURAL SERVICES	\$ 12,000.00	FY23 INSTRUCTOR SERVICES - PLAY-WELL TEKNOLOGIES CAMP
23000127	NOC ADVENTURE LLC	RECREATION, PARKS & CULTURAL SERVICES	\$ 6,000.00	FY23 INSTRUCTOR SERVICES - NANTAHALA OUTDOOR CENTER CAMPS
23000130	CLEARVIEW AI INC	PUBLIC SAFETY	\$ 5,500.00	CLEARVIEW AI SOFTWARE RENEWAL
23000134	HARDY CHEVROLET INC	PUBLIC WORKS	\$ 42,975.00	(1) 2022 CHEVROLET SILVERADO 1500
23000135	HORSE & PLOW LANDSCAPE AND CONST. LLC	RECREATION, PARKS & CULTURAL SERVICES	\$ 34,250.00	PRESTON RIDGE COMMUNITY CENTER STORAGE BUILDOUT
23000136	AQUA-NOMICS EXTERIOR CLEANING	PUBLIC WORKS	\$ 5,530.00	EXTERIOR BUILDING CLEANING OF CITY HALL AND ELECTRICAL BUILDING
23000138	VIGYAN GROUP LLC	RECREATION, PARKS & CULTURAL SERVICES	\$ 7,000.00	FY23 INSTRUCTOR SERVICES - STREM HQ TECH ACADEMY
23000139	LOCALITY MEDIA INC	PUBLIC SAFETY	\$ 28,100.00	FIRE SUPPRESSION, FIRE PREVENTION AND EMS RECORDS MGMT MAINT/SUPPORT
23000140	UGA RESEARCH FOUNDATION INC	PUBLIC SAFETY	\$ 17,255.00	PROMOTIONAL TESTING SERVICES
23000143	ANDREWS TECHNOLOGY HMS INC	FINANCE	\$ 45,669.00	NOVATIME TIME AND ATTENDANCE SOFTWARE RENEWAL
23000144	CRITICAL COMPONENTS INC	INFORMATION TECHNOLOGY	\$ 5,747.00	OEM ADVANTAGE SERVICE PLAN FOR PUBLIC WORKS DATA CENTER UPS
23000145	ANALYTICAL ENVIRONMENTAL SERVICES	PUBLIC WORKS	\$ 8,064.00	LONG TERM CHEMICAL MONITORING OF (2) STREAM LOCATIONS
23000146	ANTHONY BUDION	RECREATION, PARKS & CULTURAL SERVICES	\$ 15,091.92	FY23 INSTRUCTOR SERVICES - JIU JITSU
23000147	DOUGLAS BARTLETT ENTERPRISES LLC	RECREATION, PARKS & CULTURAL SERVICES	\$ 27,540.00	FY23 INSTRUCTOR SERVICES - SOCCER SHOTS
23000150	SUSTAINABLE WATER PLAN. & ENGINEERING	PUBLIC WORKS	\$ 20,200.00	STORMWATER MANAGEMENT FACILITY FEASIBILITY ANALYSIS
23000151	SUNBELT TRAFFIC LLC	PUBLIC WORKS	\$ 8,500.00	INSTALLATION OF (5) VEHICLE DETECTION LOPPS AT WINDWARD PKWY AND N MAIN ST
23000152	COLLECTIVE DATA INC	INFORMATION TECHNOLOGY	\$ 7,092.00	COLLECTIVE FLEET SOFTWARE RENEWAL
23000153	DARRYL D ADAMS	RECREATION, PARKS & CULTURAL SERVICES	\$ 16,209.90	FY23 INSTRUCTOR SERVICES - KARATE
23000154	PHOENIX RISING VOLLEYBALL CLUB	RECREATION, PARKS & CULTURAL SERVICES	\$ 17,550.00	FY23 INSTRUCTOR SERVICES - VOLLEYBALL
23000158	ATLANTIS PLUMBING LLC	RECREATION, PARKS & CULTURAL SERVICES	\$ 9,600.00	EMERGENCY WATER LINE REPAIR AT WILLS PARK CONCESSION BUILDING AT FIELDS 1-4
23000160	CDW LLC	INFORMATION TECHNOLOGY	\$ 9,500.00	SOLARWINDS MAINTENANCE ANNUAL RENEWAL
23000161	BOUND TREE MEDICAL LLC	PUBLIC SAFETY	\$ 30,000.00	FY23 EMS SUPPLIES
23000164	GEORGIA TECHNOLOGY AUTHORITY	PUBLIC SAFETY	\$ 25,000.00	GCIC TERMINAL FEES FOR BACKGROUND CHECKS AND THE JAIL
23000165	GULF STATES DISTRIBUTORS INC	PUBLIC SAFETY	\$ 23,900.00	AMMUNITION FOR POLICE
23000166	ATKINS NORTH AMERICA, INC	PUBLIC WORKS	\$ 35,000.00	PROJECT MANAGEMENT SERVICES FOR ALPHA LINK PRE-DESIGN SERVICES
23000168	TYLER TECHNOLOGIES INC	FINANCE	\$ 6,945.80	(10) DAYS OF PACE TRAINING
23000170	EMILY SHIVELY	RECREATION, PARKS & CULTURAL SERVICES	\$ 5,800.00	MARKETING CONSULTING SERVICES
23000173	GOVERNMENTJOBS.COM, INC.	HUMAN RESOURCES	\$ 26,268.68	HUMAN RESOURCES SOFTWARE SUBSCRIPTION RENEWAL
23000174	ATLAS GEOGRAPHIC DATA INC	INFORMATION TECHNOLOGY	\$ 9,600.00	ANNUAL MAINTENANCE OF GIS TAX PARCEL DATABASE

City of Alpharetta
Balance Sheet
Governmental Funds
July 31, 2022

	Major Governmental Funds							Non-Major	Total
	General	Capital	Capital	2016	2022	T-SPLOST	T-SPLOST II	Governmental	Governmental
	Fund	Project Fund	Grant Fund	Bond Fund	Bond Fund	Capital Fund	Capital Fund	Funds	Funds
ASSETS									
Cash / Cash Equivalents / Investments	\$ 35,588,644	\$ 9,437,700	\$ 55,899	\$ 1,000,644	\$ 29,314,779	\$ 43,183,997	\$ 3,640,539	\$ 16,104,050	\$ 138,326,252
Receivables (net of allowance for uncollectibles)									
Taxes Receivable									
Property Taxes	536,947	-	-	-	-	-	-	89,809	626,756
Other Taxes	322,866	-	-	-	-	-	-	-	322,866
Interest	-	-	-	-	-	-	-	-	-
Accounts	-	-	-	-	-	-	-	628	628
Due from Other Funds	898,507	-	-	-	-	-	-	-	898,507
Intergovernmental Receivable	15,143	240,679	178,972	-	-	843	-	3,729	439,367
Cash - Restricted	153,917	300,845	-	-	-	-	-	-	454,762
Total Assets	37,516,024	9,979,224	234,871	1,000,644	29,314,779	43,184,840	3,640,539	16,198,216	141,069,137
LIABILITIES AND FUND BALANCES									
Liabilities									
Current									
Accounts Payable	371,009	254,451	-	684,297	-	697,891	-	193,682	2,201,330
Retainage Payable	-	276,211	54,839	50,547	-	100,028	-	49,806	531,431
Intergovernmental Payable	-	-	-	-	-	-	-	-	-
Accounts payable/AR Suspense acct	-	-	-	-	-	-	-	-	-
Claims Payable	-	-	-	-	-	-	-	-	-
Payroll Payable	122,220	-	-	-	-	-	-	7,370	129,590
Due to Other Funds	-	-	-	73,498	-	823,228	-	689	897,416
Deferred Revenue	1,010,093	240,679	178,972	-	-	843	-	93,539	1,524,125
Unearned Revenue	730,018	-	-	-	-	-	-	273	730,291
Non-Current									
Unclaimed Property	122,675	-	-	-	-	-	-	-	122,675
Claims Payable	55,391	-	-	-	-	-	-	-	55,391
Total Liabilities	2,411,406	771,341	233,810	808,342	-	1,621,990	-	345,359	6,192,249
Fund Balances:									
Restricted for:									
Capital Projects	-	2,566,473	(255,487)	(50,340)	28,862,098	34,072,833	2,804,473	7,453,183	75,453,234
Law Enforcement	-	-	-	-	-	-	-	65,297	65,297
Emergency Telephone Activities	-	-	-	-	-	-	-	749,865	749,865
Grant Projects	-	-	-	-	-	-	-	-	-
Debt Service	-	-	-	-	-	-	-	327,552	327,552
Promotion of Tourism	-	-	-	-	-	-	-	945,849	945,849
Assigned for:									
Grant Projects	-	-	-	-	-	-	-	149,118	149,118
Capital Projects	-	-	-	-	-	-	-	-	-
Emergency Reserve	19,700,000	-	-	-	-	-	-	-	19,700,000
2024 Fiscal Year Capital	12,300,000	-	-	-	-	-	-	-	12,300,000
Encumbrances	4,582,983	3,413,498	265,726	124,959	390,626	6,626,571	836,066	4,139,189	20,379,618
Remaining 2023 Net Spend	(6,178,365)	-	-	-	-	-	-	-	(6,178,365)
Projected Net Surplus/2024 Capital	4,700,000	-	-	-	-	-	-	-	4,700,000
Unallocated	-	3,227,912	(9,179)	117,682	62,055	863,446	-	2,022,804	6,284,720
Total Fund Balances	35,104,618	9,207,883	1,060	192,301	29,314,779	41,562,850	3,640,539	15,852,857	134,876,889
Total Liabilities and Fund Balances	\$ 37,516,024	\$ 9,979,224	\$ 234,871	\$ 1,000,644	\$ 29,314,779	\$ 43,184,840	\$ 3,640,539	\$ 16,198,216	\$ 141,069,137

City of Alpharetta
Statement of Revenues, Expenditures, and Changes in Fund Balances
Governmental Funds
For the Period Ended July 31, 2022

	Major Governmental Funds						Non-Major Governmental Funds	Total Governmental Funds
	General Fund	Capital Project Fund	Capital Grant Fund	S2016 Const Bond Fund	S2022 Const Bond Fund	T-SPLOST Capital Fund	T-SPLOST II Capital Fund	
REVENUES								
Taxes:								
Property Tax	\$ 323,862	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ 888,307
Local Option Sales Tax	1,814,023	-	-	-	-	-	-	7,223
Transportation SPLOST	-	-	-	-	-	-	1,250,006	-
Other Taxes	587,615	-	-	-	-	-	-	319,581
Licenses and permits	731,965	-	-	-	-	-	-	21,276
Intergovernmental	18,277	38,084	87,027	-	-	-	-	-
Charges for services	599,170	-	-	-	-	-	-	-
Impact Fees	-	-	-	-	-	-	-	-
Fines/Forfeitures	370,389	-	-	-	-	-	-	31,003
Investment earnings (Loss)	94,883	27,429	315	1,931	38,780	58,954	-	4,496
Contributions and Donations	200	3,709	-	-	-	-	-	-
Misc Revenue	18,532	-	-	-	-	-	-	-
Other	-	-	-	-	-	-	-	-
Total revenues	4,558,916	69,223	87,342	1,931	38,780	58,954	1,250,006	1,271,886
EXPENDITURES								
Current:								
Unallocated	-	-	-	-	-	-	-	-
General government	1,335,254	601	-	-	-	-	-	2,915
Public safety	4,497,372	5,963	16,500	-	-	-	-	643,123
Public works	840,570	77,329	-	-	-	43,387	6,665	31,032
Economic and community development	536,814	-	-	-	-	-	-	-
Alpharetta Business Community	-	-	-	-	-	-	-	-
Culture and recreation	1,120,806	48,610	-	-	-	-	-	-
Contingency	679	-	-	-	-	-	-	-
Professional Services	-	-	-	-	-	-	-	-
Debt service:								
Principal	-	-	-	-	-	-	-	-
Interest	-	-	-	-	-	-	-	-
Other Costs	-	-	-	-	-	-	-	-
Bond issuance costs	-	-	-	-	-	-	-	-
Capital outlay	-	-	-	-	-	-	-	-
Total expenditures	8,331,496	132,502	16,500	-	-	43,387	6,665	677,070
Excess (deficiency) of revenues over (under) expenditures	(3,772,580)	(63,280)	70,842	1,931	38,780	15,568	1,243,341	594,816
OTHER FINANCING SOURCES (USES)								
Transfers in	333,115	953,317	-	-	-	-	-	-
Transfers out	(1,303,317)	-	-	-	-	-	-	16,885
Loan Proceeds	-	-	-	-	-	-	-	-
Capital Leases	-	-	-	-	-	-	-	-
Sale of capital assets	-	-	-	-	-	-	-	-
Sale of non-capital assets	500	-	-	-	-	-	-	-
Land Sale	-	-	-	-	-	-	-	-
Insurance Proceeds	-	-	-	-	-	-	-	-
Bond Proceeds	-	-	-	-	-	-	-	-
Total other financing sources and (uses)	(969,702)	953,317	-	-	-	-	-	16,885
Net change in fund balances	(4,742,281)	890,037	70,842	1,931	38,780	15,568	1,243,341	611,701
Fund balances - beginning	39,846,900	8,317,846	(69,781)	190,370	29,275,999	41,547,283	2,397,198	15,241,156
Fund balances - ending	\$ 35,104,618	\$ 9,207,883	\$ 1,060	\$ 192,301	\$ 29,314,779	\$ 41,562,850	\$ 3,640,539	\$ 15,852,857
								\$ 134,876,889

City of Alpharetta
Combining Balance Sheet
Non-Major Governmental Funds
July 31, 2022

	Special Revenue						Total Non-major			
	Hotel Motel	Impact Fee	Federal Confiscated Assets	State Confiscated Assets	Grant Operating	E911	American Rescue ACT	Debt Service Fund	Stormwater Capital Fund	Governmental Funds
ASSETS										
Cash / Cash Equivalents / Investments	\$ 1,530,638	\$ 5,145,093	\$ 136,054	\$ 34,642	\$ 174,595	\$ 1,715,666	\$ 4,222,163	\$ 1,095,792	\$ 2,049,406	\$ 16,104,050
Taxes Receivable	-	-	-	-	-	-	-	-	-	-
Pre-Paid Expenditures	-	-	-	-	-	-	-	-	-	-
Accounts Receivable	628	-	-	-	-	-	-	-	-	628
Property Taxes	-	-	-	-	-	-	-	89,809	-	89,809
Intergovernmental Receivable	-	-	-	-	3,729	-	-	-	-	3,729
Due From Other Funds										
Restricted	-	-	-	-	-	-	-	-	-	-
Total Assets	1,531,266	5,145,093	136,054	34,642	178,324	1,715,666	4,222,163	1,185,601	2,049,406	16,198,216
LIABILITIES										
Accounts Payable	-	182,032	-	-	2,100	7,404	461	-	1,684	193,682
Retainage Payable	-	24,906	-	-	-	-	24,900	-	-	49,806
Intergovernmental Payable	-	-	-	-	-	-	-	-	-	-
Arbitrage Payable	-	-	-	-	-	-	-	-	-	-
Accounts payable/AR Suspense acct	-	-	-	-	-	-	-	-	-	-
Compensated Absences	-	-	-	-	-	-	-	-	-	-
Payroll Liabilities	-	-	809	-	-	6,561	-	-	-	7,370
Due to Other Fund	-	-	689	-	-	-	-	-	-	689
Deferred Revenue	-	-	-	-	3,729	-	-	89,809	-	93,539
Unearned Revenue	-	-	-	-	-	-	-	273	-	273
Total Liabilities	-	206,939	1,498	-	5,829	13,966	25,361	90,082	1,684	345,359
FUND BALANCES										
Restricted:										
Capital Projects	-	3,748,414	-	-	-	-	2,717,053	-	987,717	7,453,183
Law Enforcement	-	-	30,655	34,642	-	-	-	-	-	65,297
Promotion of Tourism	945,849	-	-	-	-	-	-	-	-	945,849
Emergency Telephone Activities	-	-	-	-	-	749,865	-	-	-	749,865
Debt Service	-	-	-	-	-	-	-	327,552	-	327,552
Assigned for: Grant Projects	-	-	-	-	-	-	-	-	-	-
Grant Projects	-	-	-	-	149,118	-	-	-	-	149,118
Encumbrances	585,417	231,270	-	-	-	855,611	1,479,749	-	987,142	4,139,189
Unallocated	-	958,471	103,901	-	23,377	96,224	-	767,968	72,863	2,022,804
Total Fund Balances	1,531,266	4,938,154	134,556	34,642	172,495	1,701,700	4,196,801	1,095,520	2,047,722	15,852,857
Total Liabilities and Fund Balances	\$ 1,531,266	\$ 5,145,093	\$ 136,054	\$ 34,642	\$ 178,324	\$ 1,715,666	\$ 4,222,163	\$ 1,185,601	\$ 2,049,406	\$ 16,198,216

City of Alpharetta
Combining Statement of Revenues, Expenditures, and Changes in Fund Balances
Non-major Governmental Funds
For the Period Ended July 31, 2022

	Special Revenue									Total Non-major
	Hotel Motel	Impact Fee	Confiscated Assets	State Confiscated Assets	Grant Operating	E911 Fund	American Rescue Act	Debt Service Fund	Stormwater Service Fund	Governmental Funds
REVENUES:										
Hotel Motel Tax	\$ 888,307	\$ -	\$ -	\$ -	\$ -	-	\$ -	\$ -	\$ -	\$ 888,307
Property tax	-	-	-	-	-	-	-	7,223	-	7,223
Charges for Service	-	-	-	-	52,500	267,081	-	-	-	319,581
Impact Fees	-	21,276	-	-	-	-	-	-	-	21,276
Forfeiture Income	-	-	-	-	-	-	-	-	-	-
Intergovernmental	-	-	-	-	-	-	-	-	-	-
Contributions & Donations	-	-	-	-	-	-	-	-	-	-
Investment Earnings (Loss)	4,017	13,602	-	-	368	4,778	-	2,870	5,368	31,003
Other	-	-	-	-	-	-	-	-	4,496	4,496
Total revenues	892,324	34,878	-	-	52,868	271,859	-	10,093	9,863	1,271,886
EXPENDITURES:										
Tourism	-	-	-	-	-	-	-	-	-	-
Community Development	-	-	-	-	-	-	-	-	-	-
Culture/Recreation	-	-	-	-	-	-	-	-	-	-
Public Safety	-	-	13,000	3,425	-	626,698	-	-	-	643,123
Public Works	-	-	-	-	-	-	2,199	-	28,833	31,032
General Government	2,915	-	-	-	-	-	-	-	-	2,915
Debt Service:	-	-	-	-	-	-	-	-	-	-
Principal	-	-	-	-	-	-	-	-	-	-
Interest	-	-	-	-	-	-	-	-	-	-
Bond Issuance Costs	-	-	-	-	-	-	-	-	-	-
Total expenditures	2,915	-	13,000	3,425	-	626,698	2,199	-	28,833	677,070
Excess (deficiency) of revenues over expenditures	889,409	34,878	(13,000)	(3,425)	52,868	(354,839)	(2,199)	10,093	(18,970)	594,816
OTHER FINANCING SOURCES (USES):										
Transfers in / out:										
General fund	(333,115)	-	-	-	-	-	-	-	350,000	16,885
Budgeted Fund Balance:	-	-	-	-	-	-	-	-	-	-
Capital Leases	-	-	-	-	-	-	-	-	-	-
Total other financing sources	(333,115)	-	-	-	-	-	-	-	350,000	16,885
Net change in fund balances	556,294	34,878	(13,000)	(3,425)	52,868	(354,839)	(2,199)	10,093	331,030	611,701
Fund balances - beginning	974,972	4,903,276	147,556	38,067	119,627	2,056,539	4,199,000	1,085,426	1,716,692	15,241,156
Fund balances - ending	\$ 1,531,266	\$ 4,938,154	\$ 134,556	\$ 34,642	\$ 172,495	\$ 1,701,700	\$ 4,196,801	\$ 1,095,520	\$ 2,047,722	\$ 15,852,857

City of Alpharetta
Enterprise Fund -Solid Waste
Statement of Net Position
July 31, 2022

	<u>Solid Waste</u>
ASSETS	
Current Assets:	
Cash and Cash Equivalents & Investments	\$ 1,710,275
Inventories, at cost	-
Accounts Receivables (net of allowance for uncollectibles)	92,960
Prepaid Insurance Expenses	-
Total Current Assets	<u>1,803,235</u>
Noncurrent Assets:	
Restricted Cash, Cash Equivalents, and Investments	-
Total Restricted Assets	<u>-</u>
Other	-
Capital Assets	
Buildings and System	-
Machinery and Equipment	-
Less Accumulated Depreciation	-
Total Capital Assets (net of accumulated depreciation)	<u>-</u>
Total Noncurrent Assets	<u>-</u>
Total Assets	<u>1,803,235</u>
LIABILITIES	
Current Liabilities:	
Accounts Payable	4,614
Accounts Payable/ Customer Credit Balances	-
Accounts Payable/ Customer Pre-Paid Service	-
Accounts Payable/ A/R Module Suspense Acct	-
Payroll Liabilities	105
Accrued Salaries	-
Accrued Interest Payable	-
Compensated Absences Payable	-
Notes Payable - Revenue Bonds	-
Due to Other Funds	-
Total Current Liabilities	<u>4,719</u>
Current Liabilities Payable from Restricted Assets:	
Revenue Bonds Payable	-
Total Current Liabilities Payable from Restricted Assets	<u>-</u>
Noncurrent Liabilities:	
Customer Deposits	-
Compensated Absences less Current Portion	-
Revenue Bonds Payable	-
Total Noncurrent Liabilities	<u>-</u>
Total Liabilities	<u>4,719</u>
NET ASSETS	
Invested in Capital Assets, net of related debt	-
Reserved for Debt Service	-
Reserved for Encumbrances	-
Unreserved	1,798,516
Total Net Assets	<u>1,798,516</u>
Total Liabilities & Net Assets	<u>\$ 1,803,235</u>

City of Alpharetta
Enterprise Fund - Solid Waste
Statement of Revenues, Expenses, and Changes in Net Position
For the Period Ended July 31, 2022

Operating revenues:	
Charges for sales and services:	
Refuse Collection charges	\$ 9,695
Misc Revenue	-
Total operating revenues	<u>9,695</u>
Operating expenses:	
Administration	5,848,768
Non-departmental	-
Total operating expenses	<u>5,848,768</u>
Operating Gain (loss)	(5,839,073)
Non-operating revenues (expenses):	
Investment earnings (Loss)	5,138
Total non-operating revenue (expenses)	<u>5,138</u>
Income (loss) before transfers	(5,833,935)
Transfers In	-
Transfers Out	<u>-</u>
Change In Net Assets	(5,833,935)
Total net assets-beginning	<u>1,800,122</u>
Total net assets-ending (net of encumbrances)	<u>(4,033,813)</u>
Adjustments to GAAP basis:	
Encumbrances	5,832,328
Misc adj-Encumbrances Resv/Prior Year	
Total net assets-ending	<u>\$ 1,798,516</u>

DEVELOPMENT AUTHORITY



Revenue & Expenditure Report GAAP Financial Statements



ALPHARETTA DEVELOPMENT AUTHORITY

Financial Management Report - As of July 31, 2022 (unaudited)

Account #	Project	Total Budget	Actuals (Collections/ Expenditures)	Encumbrances	Remaining
Revenues					
99575100-346900	Bond Application Fee	\$ -	\$ -		\$ -
99575100-361000	Investment Earnings	-	-		-
99575100-371000-C1532	ATC Operational Funding (COA)	95,000	-		95,000
(2) 99575100-381000-C1535	Innovation Center Operations (ATC)	23,700	783		22,917
	subtotal	\$ 118,700	\$ 783		\$ 117,917
(1) 99575100-395000	Carryforward Fund Balance	\$ 214,749	\$ -		\$ 214,749
	subtotal	\$ 214,749	\$ -		\$ 214,749
	Total	\$ 333,449	\$ 783		\$ 332,666
Expenditures					
99575100-571000-C1403	Local Job Creation Grant Program	\$ 32,500	\$ -	\$ -	\$ 32,500
99575100-544100-C1532	ATC Operational Funds	95,000	15,833	79,167	-
99575100-544100-C1601	High Impact Permitting Grant Program (IGA with COA)	20,948	-	-	20,948
99575100-544100-C0924	Economic Development Strategic Plan (split with COA)	37,500	-	-	37,500
99575100-544100-C2210	Downtown Economic Development Initiative	60,000	-	-	60,000
99575100-531100	General Supplies & Materials	-	-	-	-
	subtotal	\$ 245,948	\$ 15,833	\$ 79,167	\$ 150,948
(2) 99575100-522250-C1535	Innovation Center Operations (Facility Repair & Maint.)	\$ -	\$ -	\$ -	\$ -
(2) 99575100-523860-C1535	Innovation Center Operations (Maintenance Contracts)	12,000	-	9,000	3,000
(2) 99575100-531200-C1535	Innovation Center Operations (Miscellaneous Utilities)	1,100	-	-	1,100
(2) 99575100-531210-C1535	Innovation Center Operations (Water/Sewer)	600	33	-	567
(2) 99575100-531220-C1535	Innovation Center Operations (Natural Gas)	5,000	-	-	5,000
(2) 99575100-531230-C1535	Innovation Center Operations (Electricity)	5,000	-	-	5,000
	subtotal	\$ 23,700	\$ 33	\$ 9,000	\$ 14,667
99575100-579000	Reserve	\$ 63,801	\$ -	\$ -	\$ 63,801
	Total	\$ 333,449	\$ 15,866	\$ 88,167	\$ 229,416

(1) Carryforward Fund Balance represents cash available at the end of the prior fiscal year that is programmed into the current fiscal year budget. As this account represents cash already received, there will not be actual collections.

(2) Innovation Center utilities are being funded by the Alpharetta Technology commission (ATC) on a reimbursement basis. As such, expenses will outpace budget at month end due to the billing/reimbursement delay.



ALPHARETTA DEVELOPMENT AUTHORITY
Financial Management Report - As of July 31, 2022 (unaudited)

Account #	Project	Total Budget	Actuals (Collections/ Expenditures)	Encumbrances	Remaining
Fund Balance Reconciliation					
Fund Balance (beginning of Fiscal Year)			\$ 214,749		
Revenues collected to date			783		
Expenditures incurred to date			(15,866)		
Fund Balance (current)			\$ 199,666		
Forecasted revenue collections			95,000		
Fund Balance (forecasted)			\$ 294,666		
Allocation of Forecasted Fund Balance:					
Non-Spendable (unspent/remaining project allocations)			\$ 230,115		
Spendable (available for investment by the Board)			64,551		
			\$ 294,666		

City of Alpharetta
Balance Sheet
COMPONENT UNIT-DEVELOPMENT AUTHORITY
July 31, 2022

ASSETS

Current Assets:

Cash and Cash Equivalents	\$ 81,007
Investments	-
Receivables	119,750
Restricted Cash for Bond Issuance Costs	-

Total Assets 200,757

LIABILITIES

Current Liabilities:

Accounts Payable	-
Deferred Revenue	-
Due to Other Funds	1,091
Total Current Liabilities	<u>1,091</u>

Current Liabilities Payable from Restricted Assets:

-
-

Total Current Liabilities Payable from Restricted Assets

Noncurrent Liabilities:

-
-

Total Noncurrent Liabilities

-
1,091

Total Liabilities

Fund Balance

Restricted	135,115
Unallocated	64,551
Total Fund Balance	<u>199,666</u>

Total Liabilities & Fund Balance \$ 200,757

City of Alpharetta
Statement of Revenues, Expenditures, and Changes in Fund Balance
COMPONENT UNIT-DEVELOPMENT AUTHORITY
For the Period Ended July 31, 2022

	<u>Actual Amounts</u>
Revenues	
Rent/Royalties	\$ 783
State Grant	-
Fees	-
Contributions & Donations	-
Miscellaneous Income-Interest	-
Miscellaneous Revenue	-
	<u>-</u>
Total Revenues	<u>783</u>
Expenditures	
Economic Development	95,000
Maintenance Contracts	9,000
Donation to private source	-
Utilities - Miscellaneous	33
Debt Service:	
Principal	-
Interest	-
	<u>-</u>
Total Expenditures	<u>104,033</u>
Excess (deficiency) of revenues over (under) expenditures	(103,250)
Other Financing Sources (Uses)	
Sale of capital assets	<u>-</u>
Net Change in Fund Balances	(103,250)
Fund Balance, Beginning of Year	<u>214,749</u>
Encumbrances	88,167
Fund Balance, End of Year	<u>199,666</u>

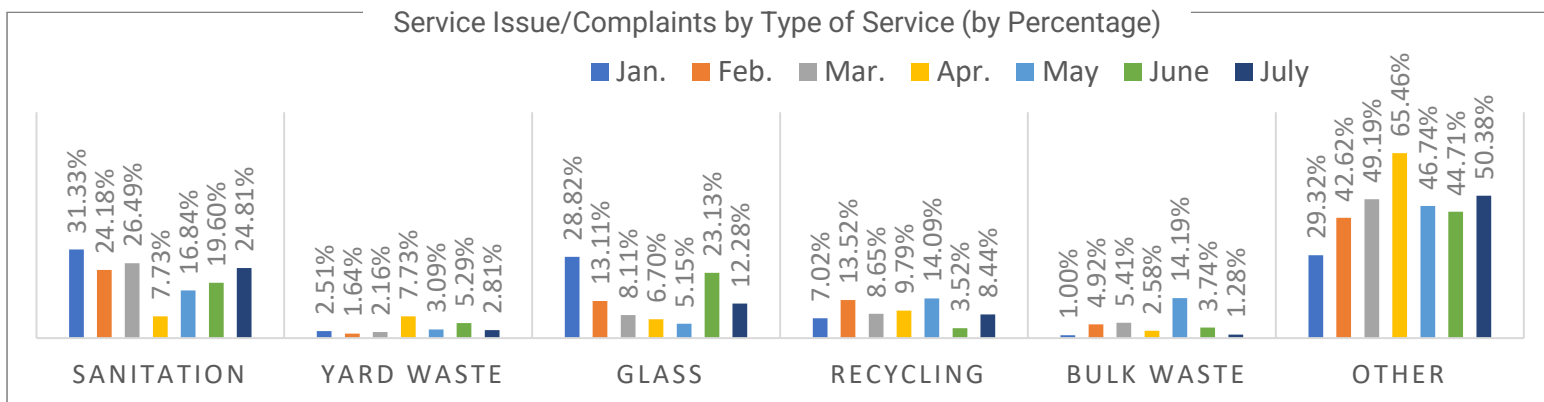
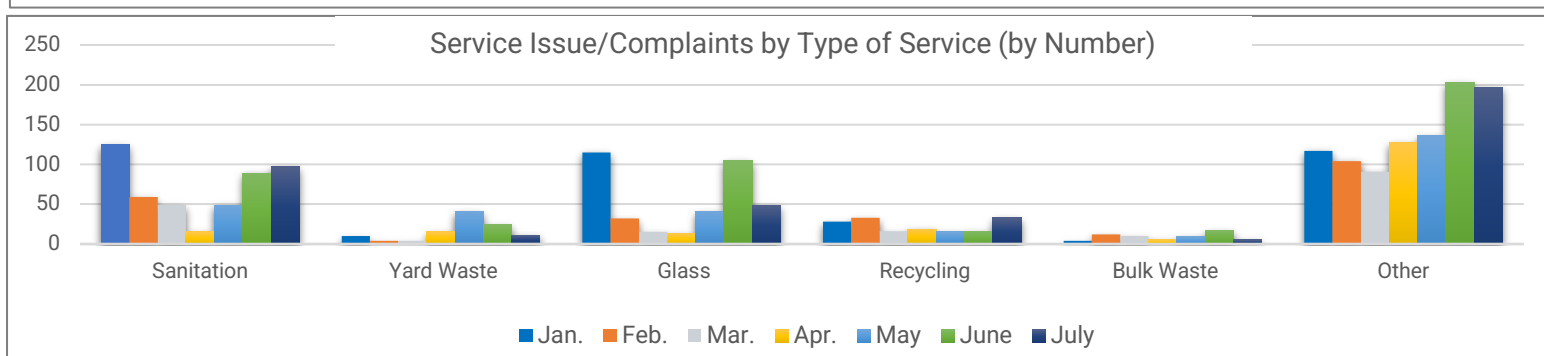
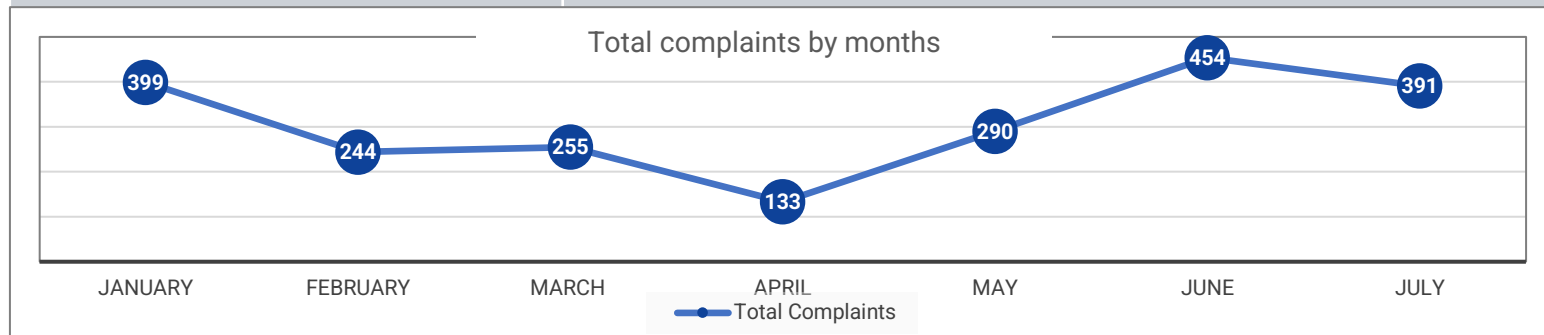


Accountability & Performance Dashboards

Republic Services –

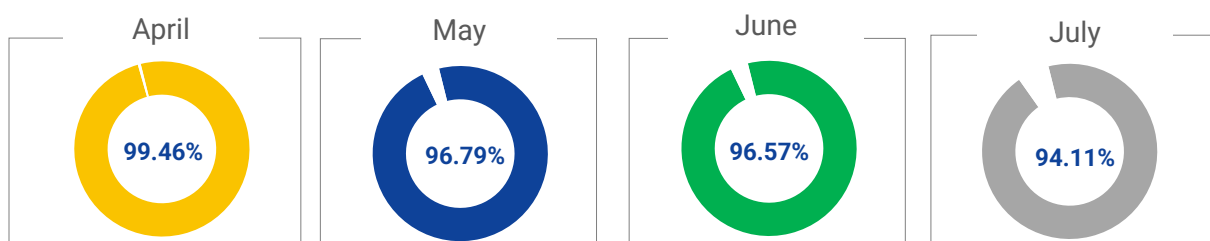
Accountability and Performance Dashboard – July 2022

Performance Measure	Purpose
Services Issue or Complaint Submission Form	Designed to allow customers to make service-related requests or raise issues such as unresolved non-operational difficulties, missed pickups, spills, etc. so that the appropriate resolution can be provided and the City/contractor can gauge service delays



Performance Measure	Purpose
Republic – Daily Route Status Updates/ routes on schedule	Status reports are provided twice a day, once in the morning and once after routes are completed for the day. Allows the City to proactively communicate information to customers if there are any incomplete/disruption in services.

Percentage of 1,120 routes collected on schedule



Taken into consideration the multiple residential services performed by Republic Services, Alpharetta residents receive roughly 360,000 touches per month (90,000 per week). Latest detail log for routes collected on scheduled on reverse side.

DISCLAIMER ON ACCURACY AND COMPLETENESS OF INFORMATION. While the CITY uses reasonable efforts to provide accurate and up-to-date information, some of the information provided is gathered by third parties and has not been independently verified by the CITY. Changes may periodically be made to the information and these changes may or may not be incorporated in any new version

This report is based on the twice daily route status emails from Republic Services. Republic Services operates thirteen to fourteen routes on most days, with Friday being a lighter day.

Route Status Report

Route Status Report – July 2022

Type of Service	Week 1:	Week 2:	Week 3:	Week 4:		Percentage OS by Type of Service
On Schedule (OS) – All Services						
Service Delay - Sanitation/Household Garbage	¼ (Fri) *	OS	OS	OS		98.75%
Service Delay – Glass	OS	2 (Thur. Fri.) *	1 ½ (Mon, Thurs) *	4 (Tues – Thurs) *		62.5%
Service Delay – Recycling	OS	OS	OS	OS		100%
Service Delay – Yard Waste	OS	OS	½ (Thurs)*	OS		90%
Service Delay – Bulk Waste	OS	OS	OS	OS		100%
Service Delay – Backdoor	OS	OS	OS	OS		100%
Service Delay – Pup Truck	OS	OS	OS	OS		100%
TOTALS (Percentage OS by week)	99.29%	94.29%	94.29%	88.57%		

Detail Description of Delays *

Week 1:

- July 5-6 - Jere street is blocked and unable to service.
- July 7 – Jere street serviced
- July 8 - End of day all routes complete. 1 trash route unable to complete due to mechanical failure...Bellflower rd. We tried to get drivers to complete the area tomorrow but were not successful. The driver who normally services the route will return on Monday to complete the route and his normal route for the day.

Week 2

- July 14 - All routes are currently on schedule. Glass truck went down. We will not be competing glass today
- July 15 – Everything was complete today except glass.

Week 3:

- July 18 - Unfortunately, we are currently not running again glass today. All other routes are running as planned.
- July 21 - Glass and yard waste that did not complete.

Week 4:

- July 26 - All routes are running today except glass.
- July 27 - All routes are running today except glass.
- July 28 - All routes are running today except glass.
- July 29 - All routes are running today except glass.





STAFF REPORT

Submitting Department: Public Works

Submitted By: Pete Sewczwicz

Sponsored By:

Meeting Date: September 26, 2022

I. AGENDA ITEM TITLE: MEMORANDUM OF UNDERSTANDING: GDOT GA 400 MANAGED LANES UTILITY

APPROVAL OF PUBLIC PRIVATE PARTNERSHIP (P3) MEMORANDUM OF UNDERSTANDING BETWEEN THE GEORGIA DEPARTMENT OF TRANSPORTATION AND THE CITY OF ALPHARETTA TO CONSTRUCT EXPRESS LANES ALONG GEORGIA STATE ROUTE 400.

II. RECOMMENDATION:

Approve the memorandum of understanding with the Georgia Department of Transportation for the GA 400 Managed Lanes Project regarding utility coordination and authorize the Mayor to execute all necessary documents.

III. REPORT IN BRIEF:

On June 15, 2022, Council approved a Memorandum of Understanding (MOU) with Georgia Department of Transportation in association with the GA 400 Managed Lanes Project. At that time, the project was structured as a Design Build Finance Maintain (DBFM) project. The project structure has recently been changed to a Public Private Partnership (P3) approach; thus, the MOU has been modified and needs to be re-executed.

The attached MOU is associated with the GA-400 Managed Lanes project and specifically refers to utility relocation at conflict points such as Webb Bridge Road and Tradewinds Parkway. In order for the developer to prepare their bid documents, the developer needs to know who is responsible for the design, construction, and materials for the cost of any utilities to be relocated. If any required utility relocation is included in the contract through a MOU with GDOT, the City would not have to pay for any of the design, construction, and materials costs.

Public Works recommends the responsibility for designing, constructing, and coordinating any City-owned utilities (traffic signal fiber, stormwater pipe, etc.) be at the expense of the developer and not the City of Alpharetta (*refer to item 3b -option 2, of the attached MOU*).

The overall goal of the utility MOU is to speed construction by allowing utility relocation to be included in the developer's bid. The MOU allows potential bidders to determine what their responsibilities are as related to utility relocation design, construction, and material cost.

IV. ALTERNATIVES:

V. ATTACHMENTS:

GDOT GA 400 MOU

Georgia DOT Project: SR 400 Managed Lanes
GDOT P.I. 0001757

PUBLIC PRIVATE PARTNERSHIP (P3) MEMORANDUM OF UNDERSTANDING

between the
Georgia Department of Transportation (hereinafter the DEPARTMENT)
and
City of Alpharetta (hereinafter the OWNER)

Whereas the DEPARTMENT proposes to procure a P3 project, hereinafter referred to as the PROJECT, to construct Express Lanes along SR 400 (PI 0001757) in Fulton and Forsyth County, Georgia as authorized by O.C.G.A. § 32-2-80; and

Whereas the DEPARTMENT will accomplish the PROJECT through (i) a developer, hereinafter referred to as the DEVELOPER, which will enter into a contract, hereinafter referred to as the CONTRACT, for the design, build and finance of the PROJECT and will subcontract certain work to a combination of contractors, design consultants (or design consultant team) and other entities; and (ii) the OWNER; and

Whereas, pursuant to O.C.G.A. § 32-6-170(b), the DEPARTMENT is authorized to pay or participate in the payment of the costs of removal, relocation, protection, or adjustment of the OWNER'S facilities, hereinafter referred to as the UTILITY ADJUSTMENT WORK, where the DEPARTMENT has made the determination that (i) the type of facility is one of those delineated in Section 1. below; (ii) such payments are in the best interest of the public and necessary in order to expedite the staging of the PROJECT; and (iii) the costs of the UTILITY ADJUSTMENT WORK are included as part of the PROJECT.

Whereas the OWNER may elect for the UTILITY ADJUSTMENT WORK to be carried out (i) by the OWNER; or (ii) by the DEVELOPER under the CONTRACT either utilizing the OWNER'S pre-approved design consultants and contractors or utilizing the DEVELOPER'S own design consultants and contractors.

1. Type of Utility

The OWNER has the following utility facilities in respect of which UTILITY ADJUSTMENT WORK may need to be carried out as a result of the proposed PROJECT:

Type of facility or facilities of the OWNER: *[Check to signify]*

- ☐ Domestic water mains and distribution lines and associated appurtenances
- ☒ Sanitary Sewer facilities and/or Storm Drainage System
- ☐ Electrical Distribution (overhead and underground) wires, poles, etc.
- ☐ Electrical Transmission (overhead and underground) wires, poles, etc.
- ☐ Natural Gas Distribution Facilities (underground)
- ☐ Natural Gas Transmission Facilities (underground)
- ☐ Petroleum Pipeline (underground)
- ☒ Telecommunications facilities and equipment
- ☐ Cable TV facilities

- ☐ Street Lighting
- ☐ Internet Data Service
- ☐ Other Facilities contemplated under O.C.G.A. § 32-6-170(b) (Description) [Click or tap here to enter text.](#)

2. New Utility Facilities Proposed (Betterment)

The OWNER desires the following to be installed as new additional facilities within the PROJECT right of way, hereinafter referred to as a BETTERMENT:

[Insert here or attach a detailed description of proposed new additional utility installations]

[Click or tap here to enter text.](#)
[Click or tap here to enter text.](#)

The OWNER acknowledges and agrees that (i) any BETTERMENT will be subject to terms to be mutually agreed between the DEVELOPER and the OWNER and documented pursuant to a separate betterment agreement between the DEVELOPER and the OWNER, a copy of which betterment agreement must be provided to the DEPARTMENT; (ii) any such BETTERMENT will be subject to the same standards and requirements as if it were necessary UTILITY ADJUSTMENT WORK; and (iii) the OWNER will be responsible for all costs relating to any BETTERMENT and the DEPARTMENT will have no obligation to pay for or facilitate any such BETTERMENT.

3. Assignment of Responsibilities for Design and Construction

The OWNER hereby acknowledges and agrees that (i) prior to the award of the CONTRACT, the DEPARTMENT will not have in its possession final plans to be utilized to determine exact locations of the UTILITY ADJUSTMENT WORK; (ii) Overhead/Subsurface Utility Engineering (SUE) investigations plans exist providing the best information and signifying the layout of known existing facilities; and (iii) the OWNER has used the SUE plans for developing its determination of commitments as indicated below.

The DEVELOPER-developed plans will be developed by the DEVELOPER and provided to the OWNER after the CONTRACT is awarded. The OWNER hereby acknowledges and agree that if option 3A below has been selected (i) the DEVELOPER-developed plans shall be used by the DEPARTMENT as the final basis for the Standard Utility Agreement; and (ii) the OWNER will enter into the Standard Utility Agreement on the basis of such DEVELOPER-developed plans.

The OWNER hereby makes the following commitments with regard to the PROJECT and the UTILITY ADJUSTMENT WORK:

- 3A. The OWNER, at the DEPARTMENT'S cost pursuant to a Standard Utility Agreement, will provide the following services in respect of the UTILITY ADJUSTMENT WORK for the properties for which it has established prior rights: *[Check to signify]*

- Design ☐
- Construction ☐

The OWNER must provide documented proof of the prior right and that documentation must be verified and approved by the DEPARTMENT prior to execution of this MEMORANDUM OF UNDERSTANDING.

- 3B. The OWNER elects for the following services in respect of the UTILITY ADJUSTMENT WORK to be included in the CONTRACT (regardless of prior rights) pursuant to O.C.G.A. § 32-6-170(b). The UTILITY ADJUSTMENT WORK will be included in the scope of the CONTRACT and the costs of the UTILITY ADJUSTMENT WORK will be included in the overall PROJECT costs under the CONTRACT:

Option 1: Work to be performed under the CONTRACT by the OWNER's pre-approved design consultants and/or contractors identified in attached "Exhibit A": [*Check to signify*]

Design ☐

Construction ☐

Option 2: Work to be performed under the CONTRACT by the DEVELOPER: [*Check to signify*]

Design ☒

Construction ☒

[*If both are checked under Option 2, please leave Exhibit A blank*]

As per this section, all work necessary for the UTILITY ADJUSTMENT WORK in accordance with the plans, when approved, shall be included in the CONTRACT and accomplished by the DEVELOPER except as follows: [*Check none or list any work items to be performed by the OWNER and identify whether such work items will be at the DEPARTMENT's cost pursuant to a Standard Utility Agreement under option 3A above or at the OWNER's cost under option 3C below.*]

None ☒

Excluded Items Click or tap here to enter text.

Click or tap here to enter text.

Click or tap here to enter text.

Comments Click or tap here to enter text.

Click or tap here to enter text.

Click or tap here to enter text.

Click or tap here to enter text.

- 3C. OWNER, at OWNER'S cost, will provide the following services: [*Check to signify*]

Design ☐

Construction ☐

The following is hereby mutually agreed to and understood by both parties:

1. The identification of existing facilities including preparation of Overhead/Subsurface Utility Engineering (SUE) investigations plans will be accomplished by the DEPARTMENT prior to award of the CONTRACT and thereafter supplemented by the DEVELOPER.
2. The DEVELOPER shall coordinate reviews of the utility relocation information and obtain acceptance from the OWNER and the DEPARTMENT when required. The OWNER shall apply for and obtain any required permits from the DEPARTMENT and perform any final design or proprietary design needed to administer its own relocation work if the work will not be included in the CONTRACT. If the preliminary plans indicate that no conflict exists, and the OWNER concurs with this information, the OWNER shall provide a letter of "no conflict" to the DEVELOPER and submit a No Conflict GUPS Permit.
3. All construction engineering and contract supervision shall be the responsibility of the DEPARTMENT and the DEVELOPER to ensure that all UTILITY ADJUSTMENT WORK included in the CONTRACT is accomplished in accordance with the PROJECT's plans and specifications. The DEVELOPER will consult with the OWNER before authorizing any changes or deviations which affect the OWNER's facility.
4. For UTILITY ADJUSTMENT WORK included in the CONTRACT, the DEVELOPER shall ensure that the design, construction, and installation of the OWNER'S facilities is performed by the OWNER'S pre-approved design consultant and/or contractor (if option 3B, Option 1 has been selected) and/or by the DEVELOPER (if option 3B, Option 2 has been selected).
5. For UTILITY ADJUSTMENT WORK included in the CONTRACT, the OWNER or the OWNER's consultant shall have the right to visit and inspect the work at any time and advise the DEVELOPER and the DEPARTMENT's Engineer of any observed discrepancies or potential issues. The DEPARTMENT agrees to notify the OWNER when all UTILITY ADJUSTMENT WORK included in the CONTRACT is completed and ready for final inspection by the OWNER.
6. Upon completion of the UTILITY ADJUSTMENT WORK included in the CONTRACT and upon certification by the DEPARTMENT's project manager and the OWNER that the work has been completed in accordance with the plans and specifications, the OWNER will accept the adjusted, relocated, and additional facilities and will thereafter operate and maintain said facilities located within the PROJECT right of way subject to the DEPARTMENT's "Utility Accommodations Policy and Standards Manual (UAM), current edition" and any agreements in effect without further cost to the DEPARTMENT or the DEVELOPER. Final acceptance of the UTILITY ADJUSTMENT WORK shall be accomplished by the execution of the Utility Facility Relocation Acceptance Form. The DEVELOPER shall provide the OWNER with a complete set of "As-Built Plans" for review and approval reflecting the UTILITY ADJUSTMENT WORK performed by the DEVELOPER. Upon completion of the Utility Facility Relocation Acceptance Form and the exchange of the final OWNER approved "As-Built Plans", the OWNER will operate and maintain the installed facilities going forward based on the date of execution of the Utility Facility Relocation Acceptance Form by the DEPARTMENT.
7. For all coordination, work, services, reimbursement, and other matters in respect of UTILITY ADJUSTMENT WORK under this MEMORANDUM OF UNDERSTANDING, the OWNER shall comply with all requirements under the DEPARTMENT'S UAM and shall cooperate with the DEVELOPER in the same manner as if coordinating directly with the DEPARTMENT in accordance with the laws of the State of Georgia, the DEPARTMENT'S UAM and any agreements in effect between the DEPARTMENT and the

OWNER. The OWNER agrees to cooperate in good faith with the DEVELOPER and to respond to all requests for information or meetings required to reach a resolution of any disputed items.

8. All UTILITY ADJUSTMENT WORK performed by the OWNER, at the DEPARTMENT's cost, through a Standard Utility Agreement under option 3A above and all UTILITY ADJUSTMENT WORK included in the CONTRACT under option 3B above shall be performed in accordance with the BUY AMERICA requirements of the Federal regulations (23 U.S.C. 313 and 23 CFR 635.410). All manufacturing processes for steel and iron products or predominantly of steel or iron furnished for permanent incorporation into the work on the PROJECT shall occur in the United States. The only exception to this requirement is the production of pig iron and the processing, pelletizing and reduction of iron ore, which may occur in another country. Other than these exceptions, all melting, rolling, extruding, machining, bending, grinding, drilling, coating, etc. must occur in the United States.
 - a. Products of steel include, but are not limited to, such products as structural steel piles, reinforcing steel, structural plate, steel culverts, and guardrail steel supports for signs, signals, and luminaires. Products of iron include, but are not limited to, such products as cast iron frames and grates and ductile iron pipe. Coatings include, but are not limited to, the applications of epoxy, galvanizing and paint. The coating material is not limited to this clause, only the application process.
 - b. A Certificate of Compliance shall be furnished for steel and iron products as part of the backup information with the billing. The form for this certification entitled "Buy America Certificate of Compliance" is attached to this MEMORANDUM OF UNDERSTANDING as "Exhibit B." Records to be maintained by the DEVELOPER for this certification shall include a signed mill test report and a signed certification by each supplier, distributor, fabricator, and manufacturer that has handled the steel or iron product affirming that every process, including the application of a coating, performed on the steel or iron product has been carried out in the United States, except as allowed by this section. The lack of these certifications will be justification for rejection of the steel and/or iron product or nonpayment of the work.

The requirements of said law and regulations do not prevent the use of miscellaneous steel or iron components, subcomponents, and hardware necessary to encase, assemble and construct the above products, manufactured products that are not predominantly steel or iron or a minimal use of foreign steel and iron materials if the cost of such materials used does not exceed one-tenth of one percent (0.1%) of the total contract price or \$2,500.00, whichever is greater.

[signature page follows]

This MEMORANDUM OF UNDERSTANDING will be incorporated into the CONTRACT by reference or exhibit.

APPROVED FOR THE OWNER BY:

(Signature)

Click or tap to enter a date.

(Date)

Click or tap here to enter text.

(Printed Name and Title)

APPROVED FOR THE DEPARTMENT BY:

(Signature)

Click or tap to enter a date.

(Date)

STATE UTILITIES ADMINISTRATOR

Exhibit A

OWNER Pre-Approved Contractor List

Company Name: Click or tap here to enter text.

Address: Click or tap here to enter text.

Phone: Click or tap here to enter text.

Contact Person: Click or tap here to enter text.

E-Mail: Click or tap here to enter text.

Company Name: Click or tap here to enter text.

Address: Click or tap here to enter text.

Phone: Click or tap here to enter text.

Contact Person: Click or tap here to enter text.

E-Mail: Click or tap here to enter text.

Company Name: Click or tap here to enter text.

Address: Click or tap here to enter text.

Phone: Click or tap here to enter text.

Contact Person: Click or tap here to enter text.

E-Mail: Click or tap here to enter text.

Please provide a minimum of three.

OWNER Pre-Approved Design Consultant List

Company Name: Click or tap here to enter text.

Address: Click or tap here to enter text.

Phone: Click or tap here to enter text.

Contact Person: Click or tap here to enter text.

E-Mail: Click or tap here to enter text.

Company Name: Click or tap here to enter text.

Address: Click or tap here to enter text.

Phone: Click or tap here to enter text.

Contact Person: Click or tap here to enter text.

E-Mail: Click or tap here to enter text.

Company Name: Click or tap here to enter text.

Address: Click or tap here to enter text.

Phone: Click or tap here to enter text.

Contact Person: Click or tap here to enter text.

E-Mail: Click or tap here to enter text.

Please provide a minimum of three.

Exhibit B

To be completed after the Project is awarded

GEORGIA DEPARTMENT OF TRANSPORTATION
BUY AMERICA
CERTIFICATE OF COMPLIANCE

Date _____

WE, _____

(UTILITY/RAILROAD OWNER)

Address:

Hereby certify that we are in compliance with the "Buy America" requirements of the Federal regulations 23 U.S.C. 313 and 23 CFR 635.410 of this project.

P.I. No.

As required, we will maintain all records and documents pertinent to the Buy America requirement, at the address given above, for not less than 3 years from the date of project completion and acceptance, if we do not provide the records and documents during invoicing. If all records and documents pertinent to the Buy America requirement are delivered during invoicing, then we will maintain all records and documents pertinent to the Buy America requirement for not less than three (3) years from the date conditional final payment has been received by the COMPANY.

These files will be available for inspection and verification by the Department and/or FHWA.

We further certify that the total value of foreign steel as described in the Buy America requirements for this project does not exceed one-tenth of one percent (0.1%) of the total contract price or \$2,500.00, whichever is greater.

Signed by _____
Title _____
(Officer of Organization)

Subscribed and sworn to me before this ____ day of _____, ____.

Notary Public / Justice of the Peace

My commission expires: _____



STAFF REPORT

Submitting Department: Information Technology

Submitted By: Randy Bundy

Sponsored By:

Meeting Date: September 26, 2022

I. AGENDA ITEM TITLE: Palo Alto Hardware Refresh

Approve the purchase and installation of replacement Palo Alto network security technology to Layer3 Communications, LLC.

II. RECOMMENDATION:

Award the purchase and installation of replacement Palo Alto network security technology to Layer3 Communications, LLC in the amount of \$214,097.00 under the competitively procured State of Georgia contract #99999-SPD-NVPUT3229-0001 and authorize the Mayor to execute all necessary documents.

III. BUDGET IMPLICATIONS:

BUDGETED ITEM: YES

FISCAL IMPACT: YES

INCLUDED IN CURRENT FY CPTL BUDGET: YES

INCLUDED IN CURRENT FY OPRT. BUDGET: NO

TOTAL PROJECT COST: \$214,097.00

APPROPRIATIONS:

<u>ACCOUNT TITLE/NUMBER</u>	<u>DOLLAR AMOUNT</u>
Data Network (30117400-542400-C0900)	\$109,264.00
Equipment Refresh (30117400-542400-C1313)	\$104,833

EXTERNAL FUNDING SOURCES:

<u>ACCOUNT TITLE/NUMBER</u>	<u>DOLLAR AMOUNT</u>
N/A	\$0.00
N/A	\$0.00

IV. REPORT IN BRIEF:

This request is to provide for the replacement and upgrade of the City's Palo Alto network security system. This layer of network protection integrates with our existing systems to provide critically needed protection. This provides greater reliability and greater efficiency for the use of network services for the City. This equipment component is scheduled to be replaced every 6 years (normal maintenance life) to provide for both reliable and efficient service.

The recommended vendor for this project, Layer3 Communications, LLC, was selected through GA State Contract #99999-SPD-NVPUT3229-0001. State contracts meet the competitive bidding requirements of the State of Georgia, so local governments that choose to leverage them have assurance that the necessary research, solicitation, and negotiation has been done. That process allows us to benefit from the competition of many bidders seeking large-volume contracts.

V. ALTERNATIVES:

NONE

VI. ATTACHMENTS:

CoA E-Verify for Palo Alto - Layer 3 Communications, CoA Firewall Cleanup and Implementation Rev 2, Advanced URL Filtering & DNS Security, PALO+ALTO+NETWORKS+INFO+SHEET+2021

CITY OF ALPHARETTA

AFFIDAVIT VERIFYING CONTRACTOR PARTICIPATION IN FEDERAL WORK AUTHORIZATION PROGRAM



By executing this affidavit, the undersigned contractor verifies its individual, firm or corporation which is engaged in the physical performance of services on behalf of the **City of Alpharetta (GA)** has registered with, is authorized to use and uses the federal work authorization program commonly known as E-Verify, or any subsequent replacement program, in accordance with the applicable provisions and deadlines established in O.C.G.A. § 13-10-91. Furthermore, the undersigned contractor will continue to use the federal work authorization program throughout the contract period and the undersigned contractor will contract for the physical performance of services in satisfaction of such contract only with subcontractors who present an affidavit to the contractor with the information required by O.C.G.A. § 13-10-91(b).

Contractor hereby attests that its federal work authorization user identification number and date of authorization are as follows:

53673

Aug 18, 2022

Federal Work Authorization (E-Verify) User Identification Number (Note: 6 to 8 Digit Code)

Date Of Authorization

Layer 3 Communications

Name Of Contractor

Palo Alto Firewall Refresh

Name Of Project

This form represents the State of Georgia provided affidavit formatted with the City of Alpharetta logo. Other affidavit forms are acceptable as long as the same information is provided.

I hereby declare under penalty of perjury that the foregoing is true and correct.

Executed On: August 18, 2022

in City: Norcross

State GA

Scott Faxon
Signature Of Authorized Officer Or Agent

Scott Faxon

Vice President of Sales

Printed Name Of Authorized Officer Or Agent

Printed Title Of Authorized Officer Or Agent

SUBSCRIBED AND SWORN BEFORE ME ON THIS THE

18

DAY OF

August

, 20 22

Connie Paylor
NOTARY PUBLIC

1/14/26
My Commission Expires On





Firewall Clean-Up and Implementation



Attention:

Erik Wideman

City of Alpharetta

2 Park Plaza

Alpharetta, GA 30009

Submitted By:

Griffin Turner

gturner@layer3com.com

Layer 3 Communications, LLC 1450 Oakbrook Drive, Suite 900

Norcross, GA 30093

6/16/2022



Table of Contents

1. Executive Summary.....	2
2. Scope of Work.....	2
2.1 Firewall Clean-Up and Review.....	3
2.1.1 Firewall Gap Assessment.....	3
2.1.2 Firewall Clean-Up and Remediation	3
2.2 Firewall Hardware Replacement	4
2.2.1 Firewall New Hardware Pre-Staging	4
2.2.2 Firewall Implementation and Testing.....	4
2.2.3 Post-Implementation Support.....	5
3. Customer Responsibilities Summary.....	6
4. Pricing.....	7



Revision History

Version	Date	Author	Sections Changed and Synopsis of Changes
1	7/7/2022	Griffin Turner	Initial Draft
2	7/21/2022	Chris Lariscy	Content Development
3	7/22/2022	Griffin Turner	Content Editing

1. EXECUTIVE SUMMARY

Starting out as a traditional hardware reseller, Layer 3 Communications founding theory was that success would be determined by our ability to deliver compelling services. For more than twenty years, Layer 3 Communications evolution has been driven by our customers. Applying our intellectual capital, defined as people, processes, and technology, to our customers' problems has transitioned us into an organization that delivers a comprehensive suite of services. These services are built around three major proficiencies: Cloud and Managed Services, Cyber Security Solution, and Complex Infrastructure Engagements.

A suburb of Atlanta, located in Fulton County, the City of Alpharetta (the City) provides municipal services for its nearly 70,000 residents. These services include Public Safety, Public Works, Municipal Courts, Recreation/Leisure, Community and Economic Development.

The City relies heavily on Palo Alto Networks' Next Generation Firewalls to provide security to their information technology assets. As part of their continuing efforts to provide a more secure and usable environment for their employees and residents, the City is undergoing a clean-up of their firewall security policies.

The City has asked Layer 3 Communications to produce a proposal for a best practice policy cleanup and firewall implementation of their Palo Alto Networks' Next Generation Firewalls. In order to address the City's requirements, Layer 3 Communications will conduct an assessment of their configuration, and evaluate log data to determine how the firewall is currently used. Once this has been completed, we will then alter the security policies to improve their efficacy, and enable the best use of the capabilities of the platform.

A detailed explanation of these services and their associated costs is included in the "Scope of Work" and "Pricing Table" sections of this document. Thank you for your continued interest in Layer 3 Communications and the products and services that we provide. We are pleased to have the opportunity to present this proposal to the City for your review.

2. SCOPE OF WORK

The following section defines the scope of work to be performed by Layer 3 Communications on behalf of the City of Alpharetta. The services performed will ensure the proper configuration and implementation of the City's Palo Alto Networks' Next Generation firewalls. There will be three phases of this professional services engagement, they are as follows:

- Firewall Policy Review and Clean-up Activities
- Firewall Hardware Replacement
- Panorama Deployment and Configuration

2.1 Firewall Clean-Up and Review

It is the goal of this portion of the project to conduct a security gap assessment on the existing firewall configuration; thereby producing a list of recommended remediation steps to clean-up the existing configurations ahead of implementing the new hardware being purchased to refresh the existing firewalls. The following sections will go into detail on this process.

2.1.1 Firewall Gap Assessment

Layer 3 Communications will review the existing configuration and firewall rulebase and provide a GAP assessment for City of Alpharetta to review and approve recommendations. The assessment will be conducted in accordance with both Palo Alto Networks and Layer 3 Communications best practices. Policies will be evaluated for permissiveness, security profile adoption as well as application adoption. Recommendations will be made to bring the configuration and rulebase in line with best practice standards. All recommendations will be reviewed with City of Alpharetta staff prior to moving into the clean-up phase of the project.

Deliverables include:

- *Report detailing findings and recommendations for remediation*

2.1.2 Firewall Clean-Up and Remediation

Layer 3 Communications will take the results of reviewing the current configuration and rule-base of the existing Palo Alto Networks firewalls and will complete the remediation recommendations outlined during the review process. Any completed remediations will be with the explicit acceptance of the City of Alpharetta staff to ensure no changes are made without proper change control and client input. Layer 3 Communications will assist City of Alpharetta staff in consolidating their existing rulebase where it is both available and make sense. Any best practice improvements will be discussed and implemented in conjunction with the City of Alpharetta team. Permissive policies will be reviewed and tightened where applicable. A maximum of 5 rules will be converted to application aware rules in conjunction with the City of Alpharetta staff. Layer 3 Communications will ensure City of Alpharetta staff understand the process of converting port-based rules to application based rules as part of this clean-up activity. As part of the clean-up and remediation activity the firewall configurations for both Public Works and Public Safety will be unified into a single configuration. The unified configuration will maintain a cohesive list of policies that apply to each datacenter's IP addressing to create a unified experience in the event of a failover incident. Any unused policies and objects will be discussed and cleaned up as necessary.

Deliverables include:

- *Consolidated rule-base where applicable.*
- *Rulebase adjusted for best practices where applicable*
- *Tightening of permissive policies where applicable*

- *Single rule-base configuration to be applied to both Public Safety and Public Works firewalls.*

2.2 Firewall Hardware Replacement

After the initial review and clean-up activities Layer 3 Communications will perform a direct configuration migration from the current firewalls at City of Alpharetta and will place the configurations on the new hardware. Pre-staging will occur to validate no hardware issues exist prior to scheduling and executing the cutover event. Post-Implementation support will be provided remotely for the business day following the cutover event.

2.2.1 Firewall New Hardware Pre-Staging

Layer 3 Communications will power-on and “burn-in” the new equipment within our lab facilities. Configurations will be pulled from the existing equipment with the creation of a change freeze window. During the change freeze window any changes that must be made due to immediate need will need to be communicated to Layer 3 Communications so the new configurations may reflect the changes. During staging design and implementation diagrams and documentation will be generated and provided to City of Alpharetta staff to ensure all parties are in agreement before proceeding to the cutover event.

Provided documentation will be delivered in the form of a detailed Visio diagram PDFs.

Deliverables include:

- *Initial Design Diagrams*
- *Implementation Plan for Standup and testing*

2.2.2 Firewall Implementation and Testing

During the implementation and testing phase of the project Layer 3 Communications will work with City of Alpharetta staff during an after hours cutover window of approximately 3-4 hours to remove the existing equipment and install the new hardware with the pre-loaded configurations from the existing equipment. Physical connections will be made to restore network connectivity and the execution of the test plan will commence. Upon successful completion of the test plan all configurations will be saved and backed-up saved offline in case of any issues.

Deliverables include:

- *Removal of existing firewalls*
- *Installation of new hardware firewalls that were previously configured*
- *Test plan execution prior to cutover and post cutover, plan is to be provided by the City of Alpharetta team*

2.2.3 Post-Implementation Support

Upon successful completion of the implementation, Layer 3 Communications will assist with troubleshooting configuration or physical connectivity issues with the newly installed updated Palo Alto Networks hardware.

Layer 3 Communications will provide a point of contact to provide remote technical support to assist City of Alpharetta for one business day immediately following the install or go-live date (to be determined) with any hardware or software issues.

Deliverables:

- *Dedicated Layer 3 Communications remote engineer for one business day following implementation date.*

2.3 Panorama Deployment and Configuration

Layer 3 Communications will assist City of Alpharetta staff in the deployment of the Panorama virtual appliance and configuration related to attaining a single point of management for both the Public Works and Public Safety firewalls via Panorama management. The following sections will detail the activities and deliverables associated with this phase of the project.

2.3.1 Panorama Initial Deployment

Layer 3 Communications will assist in the deployment of the virtual Panorama appliance and assist in configuring the management interface and upgrading the appliance to the recommended code version. City of Alpharetta staff will be responsible for the virtualization configuration of the virtual appliance deployment.

- *Deployed Panorama virtual edition configured in panorama mode with a base management configuration and on the latest recommended code version.*

2.3.2 Panorama Device Group Configuration

Layer 3 Communications will import the unified configuration from the Public Works firewall and create a new device group within Panorama to ensure all firewall policies are managed via panorama. The configuration will then be pushed back to the Public Works firewall putting it fully under Panorama management. At this point, all objects on the Public Safety firewall will be renamed with a pre-pend of "Local_". Once the prepended configuration has been applied and validated the Public safety firewall will be put under Panorama management and assigned to the unified device group. Policies will then be pushed down to the Public Safety firewall and will have it fully under Panorama management. Clean-up will then be done to remove anything with the "Local_" prefix as it will no longer be needed or referenced.

- *Unified Device Group configuration for single point of management for both firewalls.*
- *Firewalls with policies fully managed via Panorama.*

3. CUSTOMER RESPONSIBILITIES SUMMARY

In order for Layer 3 Communications to effectively provide the services for this project, we will require the assistance of the customer. The customer is responsible for providing:

- Any passwords required.
- Any specific community or naming conventions.
- Remote Access to existing firewalls
- Change Freeze window a minimum of one week before the cutover event
- Any existing network and security documentation and diagrams pertaining to the project.
- Route , ARP and MAC tables for the external and internal routers connected to the firewall
- Provide detailed test plan conforming to specified parameters
- Provide staff to perform test plan effectively and efficiently
- Scheduling outage windows (as necessary)
- Appropriate resources to configure the HyperV environment for deployment of the panorama VM
- Adequate resources within they HyperV environment of the deployment of the Panorama VM.

4. PRICING

Name: Erik Wideman

Quotation No.: COA-220721-1

Address: 2 Park Plaza Alpharetta, GA 30009

Quotation Date: 9/2/22

Telephone: (687) 297-6243

Payment: Due Upon Receipt

Email: ewideman@alpharetta.ga.us

Terms: Net 30

Valid for: 30 days

State Contract #: 99999-SPD-NVPUT3229-0001

Hardware / Software

PART NUMBER	DESCRIPTION	QTY	LIST PRICE	UNIT COST	EXTENDED COST
PAN-PA-3410	Palo Alto Networks : Palo Alto Networks PA-3410 with redundant AC power supplies	2.00	\$ 26,600.00	\$18,620.00	\$37,240.00
PAN-PRA-25	Panorama central management software, 25 devices	1.00	\$ 10,750.00	\$8,600.00	\$8,600.00
Hardware / Software SUBTOTAL					\$45,840.00

Support / Renewable Licenses

PART NUMBER	DESCRIPTION	QTY	LIST PRICE	TERM	TERM UOM	UNIT COST	EXTENDED COST
PAN-SVC-PREM-3410-3YR	Premium support 3-year term, PA-3410	2.00	\$14,370.00	1.0000	3-yr	\$13,651.50	\$27,303.00
PAN-PA-3410-GP-3YR	PA-3410, GlobalProtect subscription, 3 years (36 months) term.	2.00	\$14,600.00	1.0000	3-yr	\$10,950.00	\$21,900.00
PAN-SVC-PREM-PRA-25-3YR	Premium support 3 year prepaid, Panorama 25 devices	1.00	\$5,820.00	1.0000	3-yr	\$5,529.00	\$5,529.00
PAN-PA-3410-BND-INTEDGE-3YR	PA-3410, Secure Internet Edge (Advanced Threat Prevention, Advanced URL, Wildfire, DNS Security), 3 year (36 months) term	2.00	\$62,850.00	1.0000	3-yr	\$47,137.50	\$94,275.00
Support / Renewable Licenses SUBTOTAL							\$149,007.00

Professional Services

PART NUMBER	DESCRIPTION	QTY	LIST PRICE	UNIT COST	EXTENDED COST
L3-SEC-GAP-ASSESS	Security Professional Services - Details Defined in Scope of Work	1.00	\$ 19,250.00	\$19,250.00	\$19,250.00
Professional Services SUBTOTAL					\$19,250.00

Billing Terms: 1 One Time Bills

Total Cost: **\$214,097.00**First Bill: **\$214,097.00**

****To place this order, please sign, date, print name, and assign a PO number to this page of the proposal and fax along with a copy of your PO to my attention at (770) 225-5298.**

Advanced URL Filtering & DNS Security

Attribute	Advanced URL Filtering	DNS Security
Benign Categories	Create access policies based on the website category	
Multi-Category with Risk	Enforce selective Decryption and increased Threat enforcement based on Risk level	
Credential Theft Prevention	Protects users from submitting their corporate credentials to unapproved sites	
Malicious Categories	Full URL path malicious categorization for maximum precision. Inline ML logic to detect new and unknown phishing and malicious JS attacks.	Block malicious domains at DNS level to prevent threats over any protocol
TLS Evasion		Blocking malicious DNS resolutions prevent techniques like SNI Spoofing that can be abused to bypass Decryption controls
DNS Tunneling		Prevent attackers from stealing your data over DNS
DGA Protection		Prevent malware from using algorithmic techniques that dynamically generate domains for command-and-control callback

The most comprehensive DNS security solution available

Callback Domains

DNS-based indirection for reliable phone-home

Malware & C2 Domains

Botnet Domains

Fast-flux Domains

Random DGA

Dictionary DGA

High Risk Domains

Proactive protection from likely malicious domains

Grayware

Newly Registered Domains

Parked Domains

Proxy Avoidance

Dynamic DNS

Predictive Detection

NEW

Strategically Aged Domains

DNS Record Attacks

Domain takeovers through DNS zone hacks and abuse

Domain Squatting

Dangling DNS

NEW

Compromised DNS Zone

NEW

Wildcard DNS

NEW

CNAME Cloaking

DNS Protocol Attacks

DDoS, exploitation, and lateral movement

DNS Rebinding

NXNSAttack

Covert Channels

Abuse of DNS protocol for stealthy data theft and C2

DNS Tunneling

Ultra-slow DNS Tunneling

NEW

DNS Infiltration

★ Industry First

Industry-leading coverage across every major DNS-layer attack category.



Statewide Contract Information Sheet

Statewide Contract Number		99999-SPD-NVPUT3229-0001	NIGP Code	20458, 20464, 20664, 20928, 92037, 92005
Name of Contract	Data Communication Products & Services			
Effective Date	12/20/2019	Expiration Date	9/30/2024	
Contract Table of Contents				
Suppliers Awarded	1 Supplier Awarded	Contract Information:	Convenience Consortia	
Contract Information for Supplier			Page Number	
			2	
Additional Contract Information				
General Contract Information			2	
Ordering Instructions			3	
Contract Renewals			3	
DOAS Contact Information			3	
Authorized Reseller List by Manufacturer			See attachment	



Supplier Information Sheet

Contract Information	
Statewide Contract Number	99999-SPD-NVPUT3229-0001
PeopleSoft Supplier Number	0000640553
Supplier Name & Address	
Palo Alto Networks, Inc 3000 Tannery Way Santa Clara, CA 95054	
Contract	
Sales Dani Devito Office/mobile: 910 617 2777 ddevito@paloaltonetworks.com Contract Manager Ryan Campbell rcampbell@paloaltonetworks.com 732 516 8801 	
Contact Details	
Ordering Information	Orders are to be emailed to authorized partners. Partners can be found via link under Palo Alto Partner List. Sales contacts are listed for reference. https://www.naspo.valuepoint.org/portfolio/data-communications-2019-2026/palo-alto-networks-inc/
Remitting Information	Remit to Address: Attention: Accounts Receivable Palo Alto Networks, Inc. 3000 Tannery Way Santa Clara, CA 95054
Delivery Days	To be defined by authorized purchaser at the time of the PO issuance
Discounts	Discounts by SKU can be found on the Palo Alto price file link.
Payment Terms	Net 30 Days



Bid Offer includes	State Entities, Local Governments (County/City/Authorities) and Education (Universities/Colleges/BOEs K-12)
Acceptable payment method	Supplier will accept Purchase Orders and the Purchasing Card under this contract as permitted by current policies governing the Purchasing Card program.

Ordering Instructions:

Palo Alto Networks sells its products via a group of authorized resellers or orders can be placed directly with each one of them. Customers may choose a certified reseller from the State APPROVED RESELLER LIST. Reseller's quotation must include the Statewide Contract#99999-SPD-NVPUT3229-0001. Customers will be invoiced by the Reseller.

Please contact Ryan Campbell for additional questions.

Please use the link or check the attachments for the reseller and current price list.
<https://www.naspovaluepoint.org/portfolio/data-communications-2019-2026/palo-alto-networks-inc/>

Renewal Options: Two (2) one year renewal options.

AWARDED CATEGORIES (FOR SCOPE, PLEASE SEE ATTACHMENT B- STATE OF UTAH AGREEMENT):
 CATEGORY 1.3: ROUTERS, SWITCHES, SECURITY AND NETWORKING STORAGE

PRICING DISCOUNTS AND VALUE ADDED SERVICES (PLEASE SEE ATTACHMENT C- STATE OF UTAH AGREEMENT)

NIGP CODES:
 20458: Modems, External, Data Communications
 20464: Network Components: Adapter Cards, Bridges, Routers, Switches, etc.
 20664: Network Components: Connectors, Expansion Modules and Ports, etc.
 20928: Communications: Networking, Linking, etc. Mainframes and Servers
 92037: Networking Services, Including Installation, Security and Maintenance
 92005: Application, Infrastructure, Hosting and Cloud Computing Services, Vendor Hosted and Internally Hosted

Contract Manager: Osborne J Johnson
 osborne.johnson@doas.ga.gov
 404 232 1929



STAFF REPORT

Submitting Department: Information Technology

Submitted By: Shawn Mitchell

Sponsored By:

Meeting Date: September 26, 2022

I. AGENDA ITEM TITLE: MANAGED PRINT SERVICES, RFP 22-124

APPROVAL OF THE award of RFP 22-124 to EDGE Business Systems for managed print services.

II. RECOMMENDATION:

Please award RFP 22-124 to EDGE Business Systems for Managed Print Services at the quoted unit pricing and authorize the Mayor to execute all necessary documents.

III. BUDGET IMPLICATIONS:

BUDGETED ITEM: YES

FISCAL IMPACT: YES

INCLUDED IN CURRENT FY CPTL BUDGET: NO

INCLUDED IN CURRENT FY
OPRT. BUDGET: YES

TOTAL PROJECT COST: \$26,982. Costs for these services will vary in accordance with usage and print device deployment.

APPROPRIATIONS:

<u>ACCOUNT TITLE/NUMBER</u>	<u>DOLLAR AMOUNT</u>
Maintenance Contracts (allocated across all Departments)	\$26,982

EXTERNAL FUNDING SOURCES:

<u>ACCOUNT TITLE/NUMBER</u>	<u>DOLLAR AMOUNT</u>
-	\$0.00

IV. REPORT IN BRIEF:

The award of this Request-for-Proposals (RFP) is for managed print services. Specifically, the consumables, onsite service/maintenance, parts, etc. of our existing copier/multi-function printer fleet which consists, primarily, of 127 xerox devices across all city facilities. Additionally, the print management firm will review and advise on optimal deployment of existing print devices as well as create a replacement plan moving forward to ensure print devices are functional and poised to take advantage of changing technology.

Managed print services are funded through a per-print charge that varies by print job (e.g., black/white, color, etc.). Print management software tracks the number (and type) of print/copy jobs and that information is relayed to the managed print provider for billing.

The current provider of managed print services, 4ColorLaser, has been with the city, in some form (company ownership changed) since selection of Xerox as the print technology provider over 10 years ago. The service relationship was extended roughly 5-years ago and resulted in a net reduction in the print management per-print charge. That said, the City has had notable issues recently with print device service, consumables ordering/delivery, and overall strategic management of the print devices (roadmap for replacement of existing fleet, etc.).

RFP 22-124 was formulated by members of the Finance and Information Technology Departments and was issued in June 2022 to select a managed print services provider for a 5-year contract term that, at a minimum, accomplishes the following (scope attached):

Scope - Device Management

- Must be authorized by Xerox to service and support the entire product line.
- Must be factory trained and certified.
- Technicians must be vetted through GCIC (public safety).
 - Vendor and its employees must agree to a Non-Criminal Justice CJIS Network & Data Agreement.
 - Vendor must maintain and manage their employees' GCIC required training and provide training records upon request.
- Only genuine OEM parts and consumables will be used.
- Must have at least one physical location with OEM parts and consumables within 30 miles of Alpharetta City Hall, 2 Park Plaza, Alpharetta, GA.
- Average time between placing a service call or support email and service technician or dispatch agent response contact to Information Technology Department or point of contact at the device location will be within 2 hours.
- The City expects equipment to be repaired within one (1) day.
 - If a device cannot be repaired, a loaner device must be provided meeting the previous device's specifications as to not interrupt workflow.
- Supplies distribution chain to designated print administrators for each department.

Scope - Technology Management

- Upgrade the Print Management / Deployment Software.
 - A minimum of 1 software upgrade per year to keep up with vulnerability patches and bug fixes.
 - Software versions across all devices in the field within the respective device families need to be uniform.
 - Provide centralized security and configuration management for all devices.
- Must be able to provide Paper Cut integration and in-house support.
- Must be able to provide Azure integration and in-house support.
- Enable Find-Me / Secure Print release – Documents printed for any of the devices must be able to print to a virtual queue and have their jobs released at any device in the fleet.
- SSO Integration for Office365 Apps.
- Secure badge release printing using badge ID integration within AD via our future Badge management system Avigilon.

The City's procurement software detailed over 450 vendor invites and 45 document takers for RFP 22-124.

Proposals were received on July 21, 2022, by two firms:

- 4ColorLaser (current vendor)
- EDGE Business Systems

An Evaluation Team comprised of representatives from the Information Technology and Public Safety Departments reviewed the proposals based on the criteria provided in the RFP which includes:

- Technical Proposal (70 points)
 - Compatibility with Functional and Technical Requirements
 - Proposed Staffing Approach
 - Company Background, Experience, Client References, Customer Service Rating

- Cost Proposal (27 points)
- Local Vendor Preference (3 points)

The resulting scores from the Evaluation Team are as follows:

- EDGE Business Systems (73.66 points)
 - Technical: 58.75 points (out of max of 70)
 - Cost: 14.91 points (\$26,982 annual estimated cost)
- 4ColorLaser (61.38 points)
 - Technical: 34.38 points (out of max of 70)
 - Cost: 27 points (\$14,904 annual estimated cost)

The Evaluation Team recommends awarding a 5-year contract for managed print services (RFP 22-124) to EDGE Business systems. EDGE scored significantly higher on the technical components of the RFP and their cost is less than what the City is currently paying for many of the print devices in our fleet. Team members contacted references for EDGE which highlighted excellent service levels and a responsive management team.

V. ALTERNATIVES:

VI. ATTACHMENTS:

1-EDGE Cover Letter, bussiness in, 1-EDGE Technical Response Pg, BAFO EDGE RFP 22-124 Print Fleet Monthly Usage Pricing W-O PaperCut, RFP 22-124 Scope of Work-Proposal Submission, RFP 22-124 Managed Print Services - Record of Receipt

July 20, 2022

City Of Alpharetta
2 Park Plaza
Alpharetta, GA 30009

Re: City of Alpharetta Managed Print Services RFP

EDGE Business Systems is pleased to present our proposal to the City of Alpharetta for the management, support, service and supplies for the Xerox Multi-Function Color, BW Xerox Copier/Printer RFP fleet.

Founded by a management team with more than 70 years of industry experience, in 2012, EDGE Business Systems is a leading provider of document technology solutions to businesses in the Greater Atlanta area. Combining award-winning service with the latest and best in office technology, we help our clients achieve maximum productivity.

As one of the largest and fastest growing independent printer and copier dealers in Georgia, EDGE has earned recognition from manufacturers, industry insiders and publications for our continued excellence. We also offer a range of services and solutions that enable you to optimize your document processes and IT infrastructure.

Our expertise are in the Managed Print Services Sector and our *MEASURE/SIMPLIFY/MANAGE/SECURE* process is highlighted on all our trucks, technician vehicles, and billboards.

With our constantly growing staff of almost 100 employees, EGDE Business Systems has made significant investment in software specific to assessing print/copy/scan environments. Our CRM, SHERPA, has been designed specifically for Managed Print Services.

EDGE Business Systems is the outright leader in MPS in the Southeast.

Eric Denny is dedicated to maximizing customer satisfaction in the Government space and he will be the primary point of contact and dedicated project manager.

We are grateful for the opportunity to compete for the service business with one of the most revered municipalities in Georgia, The City of Alpharetta.

We look forward to a long-term business partnership between our two great organizations.

Kind Regards,

Eric Denny – Cell (770) 882-3084 / Office (404) 228-4951x104
1350 Northmeadow Pkwy, Suite 130
Roswell, GA 30076
edenny@edgeatl.com

City of Alpharetta RFP 11-124 Managed Print Services Response by EDGE Business Systems
Managed Print Services Recommendation

Further to our recent review regarding your requirements, we are pleased to enclose our recommendations to provide The City of Alpharetta with a Managed Print Services plan that fully meets the stated requirements for your Xerox Printer and Multi-Function Device fleet. As one of the largest independent dealers in Georgia, with our headquarters only 2.2-miles from Alpharetta City Hall, EDGE has earned recognition from manufacturers, industry insiders and publications for our continued excellence. We also offer a range of services and solutions that enable you to optimize your document processes and IT infrastructure.

Our strategy for the City of Alpharetta is to capitalize on the combined strength of EDGE Business Systems, PaperCut, and Xerox. EDGE Business Systems will be responsible for all delivery, installation and setup, maintenance and support, and customer services for the fleet and the PaperCut software proposed. Xerox serves as our comprehensive resource for their full line of award-winning office equipment and program support. We look forward to establishing a winning partnership with the City by providing:

- PaperCut, the best Print Management Software for your requirements
- All EDGE Technicians who are factory trained and certified by Xerox
- Consistent billing with one invoice managed systems
- Active Account Management
- Ease of use with initial and ongoing support
- Improved cost control and easy device management
- Service Level Guarantees to average 3.01-hour response with 99.2% uptime

Kindest Regards,

Eric Denny – Government Account Executive

EDGE Business Systems

1350 Northmeadow Pkwy, Suite 130

Roswell, GA 30076

Included in our Offering

- Maintenance includes all warranty service, standard break-fix maintenance and service, emergency service calls, parts and labor, and all supplies (excluding paper and staples)
- Delivery, professional installation of PaperCut by the EDGE application specialist, Matt Park, and set-up to existing network, and user-training
- Tier 1 PaperCut support is handled by the internal EDGE team with 3 certified PaperCut technicians
- Telephone and onsite support Monday through Friday, 8:00 am to 5:00 pm Local Time
- Average of 3.01-hour response with 99% uptime measured quarterly throughout Georgia
- 95% average fleet uptime measured quarterly
- All EDGE technicians are Xerox Factory-trained and certified to support all service requests on the full Xerox product line
- Customized web portal for asset reporting and service and supply requisitioning
- Data capture and reporting capabilities to remotely monitor and manage the City of Alpharetta fleet
- FM Audit Software customized for EDGE MPS program – automatic meter reporting and automatic toner Replenishment to end use

EDGE Managed Print Services Account Management Process

MEASURE - Consistently auditing the current print environment. Identify all network devices' make, model, usage, and trends. Create a baseline for potential upgrade without increasing spending. Capture all cost associated with document creation.

SIMPLIFY – Vendor consolidation. Central Management & Customize Invoicing. Realign overall document technology strategy. Right-Sized new solution with consistent manufacturer, make & model.

MANAGE – Continued recommendations based on the changing needs of your organization's environment. Ongoing quarterly reviews & recommendations regarding scanning workflows & document process automation. Discuss impact of any changes on your document workflow.

SECURE – Compliance recommendations & device authentication. Confidential and auditable print and scan. Multiple options for deployment of mobile print. Single Sign On (SSO) and dashboard reporting individual metrics.

City of Alpharetta Scope of Work

Minimum Requirements

- A. Edge Business Systems is authorized by Xerox to service and support the entire product line.
- B. All EDGE Business Systems' 18 technicians are Xerox factory trained and certified.
- C. EDGE Business Systems conducts background checks before hiring any person. We will comply and have all employees that may ever be involved with the City of Alpharetta vetted.
- D. As a Xerox premier partner, EDGE Business Systems can only use only OEM parts and consumables.
- E. EDGE Business Systems Headquarters is located 2.2 mile from Alpharetta City Hall. EDGE has a 2nd warehouse for parts, located 3.1 miles from Alpharetta City Hall, in addition to 2 satellite offices, 1 in Athens, Georgia, 1 in Dalton, Georgia. 85% of EDGE Business Systems staff is located at our Headquarters in Roswell.
- F. The primary software proposed for this project by EDGE is PaperCut. Matt Park, EDGE Business Systems Application specialist, will install, train and support PaperCut. In addition, we have 3 members of our technical support staff that are certified by PaperCut. EDGE Business Systems is the only company in the Greater Atlanta area to provide TIER 1 support for PaperCut. If at any time EDGE contacts PaperCut for support, we're directly sent to TIER 2 support. More information on this is on Matt Park's bio.
- G. The average time between placing a service request and the dispatch agent responding, either via our local phone number at 404-228-4951 or via our customer web portal is 11 minutes. Our average on-site service response time for our large service coverage area encompassing all Northwest Georgia is 3.1 hours. With the City of Alpharetta offices located within a 5-mile radius of EDGE Business Systems HQ our average response time will be significantly less.
- H. EDGE has proudly overstaffed our service team with one technician per 350 machines in the field. This has allowed us to achieve a documented 3.01 hour restore time, 99.2% equipment uptime and 86% first time fix rate (industry average is 75%) for major corrective maintenance. For minor corrective maintenance, remote resolution is available via our IT Services Help Desk. Issues that relate to being minor, for example, are settings related to scan to email/folder, address book and follow me printing settings. These are known as 'network' or 'application' issues, not 'hardware', and require assistance from a different technician, an IT Technician.
- I. In the occasion that EDGE Business Systems is not able to close a call within a day, upon request, EDGE Business Systems will provide a loaner of equal or greater capabilities at no cost to the City of Alpharetta. The loaner will be left on-site until any issues with the equipment that is down are completely resolved and the resolution is accepted by the City of Alpharetta.

i. **Supply Distribution – EDGE Automatic Toner Replenishment Program (ATR)**

To avoid business interruptions, EDGE Business Systems has put in place an Auto Supply replenishment process. When a supply item, such as toner reaches 25% level, the toner is automatically shipped. This is our process:

Automated Replenishment

- Toner arrives “just in time”
- No need to order via GSP unless specified as “Manual Order”
- Shipping Labels
- Device data/location printed directly on Shipping Label
- Internal Location (*office/cube #, role/name*)
- Serial #
- Make/Model
- Asset # and/or Cost Center
- Primary Site Contact

A. Technology – EDGE’s proposed Print Management Software solution, PaperCut, will not interfere in any way with PrinterLogic remote driver installation process. PaperCut does include remote driver installation as well. All PaperCut collateral material requested will be on a separate PDF named **ATTACHMENT 1**. The PaperCut solution proposed by EDGE Business Systems includes quarterly upgrades, including vulnerability patches and bug fixes. PaperCut includes SSO integration with Office365 and One Drive for Business.

PaperCut has Enable Find-Me / Secure Print release with SSO authentication to the device via the City of Alpharetta user Active Directory credentials and is compatible with the Avigilon Badge Management System. The pricing provided will have a separate line item for adding Badge Readers to existing Xerox equipment fleet. Additional functionality included in the PaperCut solution proposed will be on ATTACHMENT 1.

PAPERCUT MF – All collateral material is provided is on ATTACHMENT A. This proposed solution will meet and exceed all the City of Alpharetta requirements on section **a/b/c/d**. Additional information on this is provided below and in attachment A.

Matt Park, EDGE Business Systems Application specialist, located in our Roswell HQ, will install, train and support PaperCut. In addition, we have 3 members of our technical support staff that are certified by PaperCut. EDGE Business Systems is the only company in the Greater Atlanta area authorized to provide TIER 1 support for PaperCut. If at any time EDGE contacts PaperCut for support, we’re directly sent to TIER 2 support. Please see Matt Park’s Bio for additional information and benefits. EDGE Business Systems has had the largest amount of PaperCut placements in 2018, 2019 and 2021 of any Office Equipment Dealer in the State.

B. Proposed Staffing Approach

Team Leader – Rich Simons, Partner, VP of Sales

Project Manager and Primary point of Contact – Eric Denny, Government Account Executive.

Software Specialist that will be installing, deploying, and training the proposed PaperCut solution – Matt Park, Application Sales Consultant.

Service Contact – Brian Eife, Director of Service

Brief 1-Page Resumes:

RICH SIMONS—CO-FOUNDER & PARTNER

A registered professional engineer, Rich Simons started his career in the land development industry in 2001. He honed his analytical skills and developed his consultative approach to working with clients in that field. Foreseeing the downturn in the real estate market, Mr. Simons entered the document imaging industry in the 2007. His experience translated wonderfully to the highly transactional nature of this industry.

With his engineering and analytical background, Rich Simons was the architect for our Manage Print Services offering in place: MEASURE/SIMPLIFY/MANAGE/SECURE Process.

Mr. Simons holds a bachelor's degree in Civil Engineering from Auburn University. He lives in Roswell with his wife and three children.

ERIC DENNY-GOVERNMENT ACCOUNT EXECUTIVE

Eric has been with EDGE 2 and a half years and has over 23 years of experience in the Document Imaging Business. He has over 16 years' experience in working specifically with State and Local Government sector. He has been a trusted consultant for organizations, large and small, with a focus on State and Local Government Agencies by:

Effectively and strategically recommend office technologies and document solutions to maximize the ROI on the technology investments.

Analyzing internal business processes to automate document workflows and maximize the time dedicated to mission critical objectives.

Asses in-place MFP/printer fleets to reduce costs and meet the security and regulatory requirements for future initiatives.

Eric has worked with several local Cities, including City of Atlanta, Woodstock, Duluth, Canton, Kennesaw, Decatur, Fayetteville, Hapeville, Union City, Fairburn and Dunwoody among others. He managed the Georgia Sharp Statewide Contract from 2008 until 2016. His extensive experience working within the Georgia Government Sector gives him a unique understanding on the municipal document technology processes and needs.

Eric Denny holds a bachelor's degree in Business Administration from Florida State University. He lives in Cumming with his wife and daughter.

MATT PARK-APPLICATION SALES CONSULTANT

Matt has been with EDGE for nearly 5 years and has over 18 years of experience in the Document Imaging Business. Matt has the unique experience of being in just about every position in the industry. Starting as a Service Dispatcher, he moved on to roles as a Service Technician, Application Consultant, and Major Account Sales Director. Because of this unique experience, he truly knows how to recommend and implement the right solution.

Matt is certified through ACDI in PaperCut having been through their Technical Certification Process. Not only is Matt certified, but he is also supported by a team of PaperCut certified technicians. While Matt typically does the initial installation and configuration, he relies on EDGE's 3 certified technicians for ongoing Tier 1 support for our PaperCut clients. Additionally, due to the large number of PaperCut implementations we support, even our technicians who are not certified have hands on knowledge of PaperCut.

Because of the team's extensive knowledge and experience with PaperCut, we are afforded the benefit of receiving Tier 2 support immediately from our Authorized Service Center partner. Regardless, EDGE team members are always involved in any issues eliminating the typical finger pointing between software and hardware vendors. EDGE is your single point of contact, never a third party.

Matt Park holds a bachelor's degree from Vanderbilt University. He lives in Cumming with his wife and two sons.

BRIAN EIFE—SERVICE DIRECTOR

Brian Eife brings more than 30 years of experience in service and customer relations to EDGE Business Systems. He has worked in all facets of the industry from technician to supervisor. He has 12 years of management experience and won eight Technician of the Year awards for his technical expertise and customer service skills.

Brian holds an electronic degree from Lee Technical Institute. He lives with his wife and son in Cumming, Georgia.

C. Proposal Response Requirements

Invoice Requirements – EDGE Business Systems has 3 in-house contract administrators to manage the contract set-up, billing, and customized invoicing based on the customer requirements. One of the three internal contract/billing/invoicing administrator will be assigned to the City of Alpharetta. The typical Office Equipment dealers and manufacturers do not have this position in place. They depend on the vendors' administrative staff to handle their duties on top of site contract administrator.

D. Volume Reconciliation – The copy/print volume will be reconciliated on a quarterly basis as requested.

E. Active Account Management with reporting and quarterly reviews – This process is in place through our Managed Print Services process detailed on page 2:

MEASURE/SIMPLIFY/MANAGE/SECURE This proven process has been in place at EDGE Business Systems since 2014. **Attachment 2** will have an actual quarterly review report.

F. EDGE Service Response and Resolution Process Details

- **Tech to Machine Ratio:** EDGE boasts a ratio of one (1) technician per 350 machines in the field. The industry average is one (1) per 650, respectively. This means faster and more detailed attention on every service call as your technician simply has more time.
- **Response Time:** Average 3.1-Hour Response Time for our extensive service area in North Georgia. With our headquarters only 3-miles away from The City of Alpharetta, the EDGE Guarantee of under 4.0-hour response time will be consistently and significantly be beat
- **First Time Fix Rate:** With an industry average of 75%, we have resolved all calls with 86% accuracy on the very first call a technician arrives to the customer's facility. The reason is that EDGE overstaffs our service and support team while having technicians carry frequently replaced parts in their EDGE Vehicles.
- **Remote Firmware Updates:** Stay up to date on the latest versions of firmware
- **Remote Servicing:** EDGE will be able to access your machine remotely to decrease downtime and optimize response time
- **Immediate Dispatch to Technician:** EDGE will automatically route your service call to the technician closest to you at that time to ensure we meet our guaranteed response time
- **Immediate Service Response:** EDGE will respond immediately after a service call is placed with a generated email letting you know a technician is on their way

G. Order and Fulfilment Process – This information is described in detail on section I, item i.

H. Proposed Print Management Software – PaperCut MF – As an independent Office Technology dealer, EDGE Business Systems has the flexibility to partner with any software company that it chooses to, instead of being tied to only 1 proprietary solution. With the existing Xerox fleet and the City's technology initiatives, current and future, we believe that PaperCut MF is the best available solution in the marketplace to meet and exceed all the City of Alpharetta requirements. It will not interfere with PrinterLogic in any way. PaperCut does have the remote driver installation functionality included in the offering. More detailed information on PaperCut MF will be on **Attachment 1**. It is fully compatible with the badge integration from Avigilon. Pricing provided will have a separate line item to retrofit current Xerox MFPs with card readers that will integrate with Avigilon and the City of Alpharetta AD.

I. Exceptions – The only exceptions EDGE will have will be for Xerox equipment that doesn't have the latest security and compliance protocols and have been discontinued long enough to make it difficult for EDGE Business Systems to meet stated SLA (Service Level Agreement). The Xerox ColorQubes in place with the city will fall in that category. They will not meet the latest security compliance protocols and have been discontinued by Xerox. EDGE Business Systems will not take over management of any systems that does not have the latest security compliance protocols in place.

K. PaperCut MF – Please see attachment 1

C. Company background, experience, client references, customer service rating

EDGE Business Systems has been Georgia's fastest growing independent office equipment dealer since its inception, in March of 2012. With 87 employees, we work with organizations of all sizes, throughout the Georgia area, and around the country, to help manage their print, copy and scanning needs, with our Headquarters in Roswell, Georgia and offices in Athens, Georgia and Dalton, Georgia. The EDGE management team has over 70 years collective experience delivering managed print services to Atlanta based businesses. EDGE has received national recognition from technology manufacturers, industry experts, and industry publications, for Excellence in Sales, Service and Customer Support.

EDGE is the current and five-time **XEROX "Dealer of the Year"** which recognizes the top dealer in terms of Service Excellence, Hardware, and Services Revenue. EDGE manages over 7,500 devices locally and nationally and is the chosen partner for over 3,200 customers.

Our vision revolutionizes the way all organizations Measure, Simplify, Manage and Secure their document technologies with the best people, equipment, service, and software available in the industry to exceed customer satisfaction by investing in the best internal systems to accomplish this.

At EDGE we stick to what we know best, printers and MFPs. As many other large competitors in our industry, seeing the reduction of printing, have migrated their resources to Managed Network Services.

Alpharetta City Hall is under 3-miles from our Headquarters in Roswell and all personnel assigned to this project are at our Roswell Headquarters.

The single point of contact for the City of Alpharetta RFP is Eric Denny.

EDGE Nationally Recognized, Award-Winning Customer Service

- **Inc 5000 Award Winner:** 2017, 2018, 2019, 2020
- **5-Time Xerox National Dealer of the Year:** Multiple year Xerox Document Technology Partner of the Year
- **ENX Elite Dealer 2018, 2019, 2020, 2021:** Annual “Who’s Who” of the office technology dealer community, which is published annually, selected based on numerous criteria, including growth initiatives, innovative marketing programs, outstanding customer service, charitable contributions to the community, progressive workplace cultures and adaptability to an ever-changing market.
- **Trust Dale:** Only Local and well-respected Consumer Advocate Validation
- **94.97 2022 YTD Net Promoter Score:** Many companies claim that they have the "Best service in the business" but few even have a way to measure how happy customers are. Here at EDGE Business Systems, we have a system that allows us to capture feedback after every service call. We use the Net Promoter Score system (www.netpromoter.com) verification by CEO Juice, Inc which has been adopted by 70% of Fortune 1000 companies. This data and documentation give EDGE the advantage to close out service calls proactively and thoroughly through post-call surveys. These surveys give EDGE feedback on how the call went and how the experience was with the end user

The average North American company has a Net Promoter Score® of 30. Some well-loved companies reach scores into the 70s and 80s. Our YTD Net Promoter score of 94.97 ranks us **91** in North America, regardless of industry.

EDGE Business Systems References with the similar size and scope to the City of Alpharetta Fleet

OGLETHORPE University

Julia Rodriguez (IT Director)

jrodriguez1@oglethorpe.edu

(Phone) 404-261-1441

Southwest Communications

Eric Jones (IT Director)

Eric.Jones@swc.net

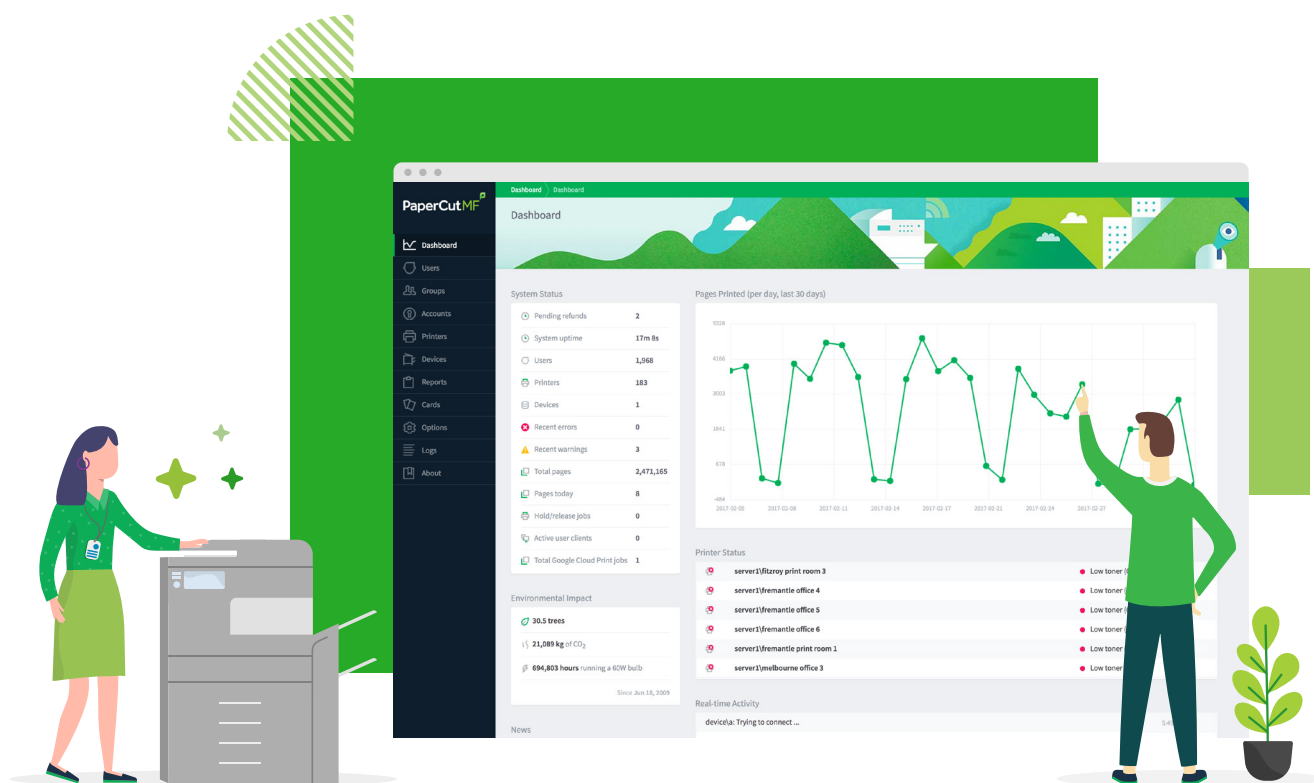
(Cell) 678-630-0870

Dalton Wholesale Flooring

Chad Templeton (VCIO)

ctempleton@armornetworks.com

(Cell) 770-891-3082



A HIGH-LEVEL FEATURE GUIDE FOR CUSTOMERS

Complete **visibility and control** of your print environment

A powerful print management solution to enable, track, manage, and secure your printing, copying, and scanning.

QRDOC.IO



v1.0

It doesn't matter what size you are, what printers you use, or what operating system your users prefer – PaperCut MF is for you.

That's because we take a cross-platform, vendor-neutral approach to technology and device support to deliver a print management solution that just works.



With PaperCut MF you can:



Manage your print environment



Save money and the planet



Secure your printing



Integrate with third-party systems



Manage 3D printing and Print Rooms



Give users power



Digitize documents

Manage your print environment

Web-based admin dashboard

PaperCut MF provides built-in, browser-based administration access from any network location to enable centralized management of every user and printing device.

[The dashboard](#) gives an easy-to-read, single-page view of the printing environment in real time, including system activity, printer error notifications, toner levels, trend information and statistics – even environmental impact. You can designate automatic quotas, deploy print queues in bulk, enable language options, and apply many more features in the pages to come.

User sync

PaperCut MF synchronizes user and group information from sources such as Windows Active Directory, Google Cloud Directory, Azure Active Directory and LDAP. This simplifies the administration of the system because you don't need to manage a separate database of users and groups.

If a user is added to the domain or is removed from a group, PaperCut automatically synchronizes this information without any intervention from the administrator. And don't worry: you can mix and match multiple sync sources for ultimate flexibility.

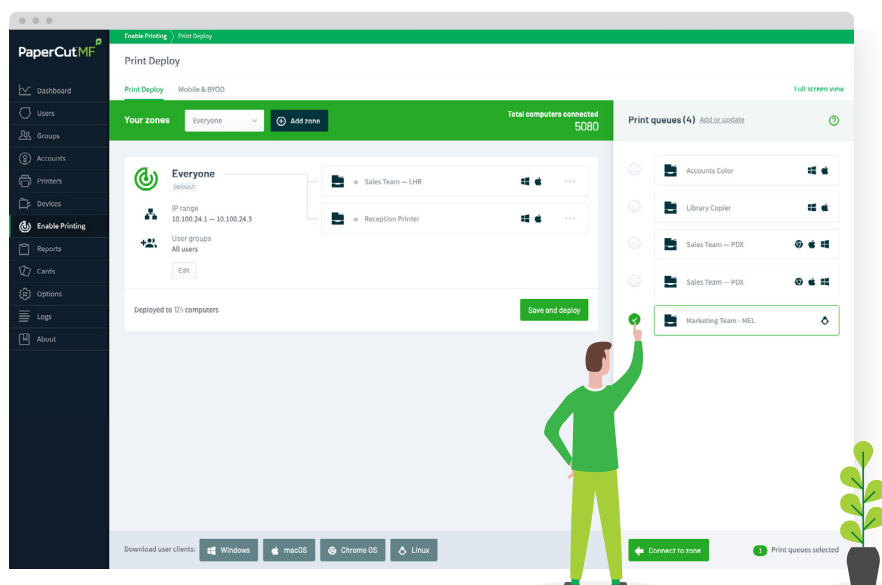
Print Deploy

PaperCut's Print Deploy feature is an innovative print queue deployment tool, allowing you to get the right print driver and right queue to the right person in the right location, automatically.

Print Deploy automates the time consuming, frustrating tasks of setting up print queues and deploying print drivers on computers in your network. Once a user leaves a site, it removes the queue and driver automatically, so clean up is a breeze.

With Print Deploy, you'll:

- ▶ Save time by deploying print queues and drivers easily at scale
- ▶ Maintain flexibility with a tool that supports environments with or without a print server
- ▶ Reduce support tickets with an automated printer configuration that's no touch for end users, even as they move between sites
- ▶ Save money on maintaining and supporting an on-premise Active Directory just to support printing
- ▶ Increase end-user productivity with automated setup and printing that just works
- ▶ Remove risk because it's from an organization with 20 years' experience in print management



Mobile printing and BYOD

Your team wants to work on the device they're most comfortable with – laptop, tablet, or smartphone; running iOS, Android, Chrome OS, Microsoft Windows or macOS – and PaperCut supports them all with its [BYOD](#) (Bring Your Own Device) features.



[Mobility Print](#) is the flagship solution for mobile printing and BYOD, enabling millions of users to easily print from their devices, with a native print experience from any application. It takes away the complexities when working across different operating systems, file formats, and brands.

Additionally, the [Web Print](#) option gives users easy access to print Microsoft Office, PDF, and image files directly from the browser, even when they're not on site or connected to the local print network. Combine this with [Email to Print](#), and users have the option to email their jobs to an address you create (e.g. printme@organization.net), and their documents will print at an authorized printer within your environment, making guest printing as easy as PaperCut.



Save money and the planet

Reporting

PaperCut MF includes over 80 one-click [reports](#) available for online viewing, export, or print. Reports address all areas, from detailed page logs to summaries by user, department, device, and environmental impact.

Administrators can also build custom reports to make sure they're delivering the most applicable data; and all these reports can be emailed to specific people on a regular schedule, removing any manual efforts.

Print policies

Implementing a print policy isn't just about sending people an email with a list of rules to follow; a great policy is automated through a system. Enter PaperCut MF.

[Print policies](#) allow you to track and control printing and copying based on users, department, class, or client. Start out lightly by suggesting environmentally friendly printing options like double-sided or grayscale printing, or add firm rules to restrict behavior and reduce waste.

Advanced scripting

[Advanced scripting](#) can be used to define and fine-tune your print and copy policies, and support your organization in eliminating waste and changing user behavior.

With advanced scripting, you can:

- ▶ Route complex jobs to more efficient, high volume printers
- ▶ Display a pop-up message if a user forgets to select duplex or grayscale
- ▶ Restrict users' functionality (e.g. after hours)
- ▶ Allow free printing on schedules (e.g. during class or workshop times)
- ▶ Give discounts during off-peak times
- ▶ And much more...

Cost recovery

Want a bigger impact than just applying policies? Designate different [costs for print settings](#), such as color versus grayscale, single-sided versus duplex, and printer P versus printer C.

User pay-for-print

Set users or groups up with [quotas](#) by applying credit to their account. This can be a recurring allocation per semester, quarter, month, or hour – or even implement a “use it or lose it” policy.

Integrate with one of many third-party payment gateways – such as PayPal, Authorize.Net, RBS WorldPay and CyberSource – to enable users to transfer balance directly from their bank to their PaperCut account.

Or give users quick and easy print credit by using [prepaid/top-up cards](#). Create a bulk batch and distribute them to different department heads, or offer them in a vending machine. A user buys a card, enters the unique code into their PaperCut UI, and ta-da: they're ready to print!



Client Billing

Are you printing in a business that would like to bill costs back to a client or project? That's easy with PaperCut MF's [Client Billing](#). Every time a job is initiated, select the appropriate account and the charge will be applied to their balance, making tracking and invoicing simple and precise.

To make things extra easy, PaperCut integrates with a variety of third-party legal and accounting systems so you don't even need to change your existing setup to start feeding data through.

Secure your printing

End-to-end encryption

PaperCut MF supports end-to-end encryption on the network. That means not just security at the printer, but from the user's device to the print server, the print server to the printer, and the printer to the user's hand. They're protected at every stage, from "I want to print this," to "I've printed this, now it's time for coffee."

User authentication

To avoid mix-ups with balance allocations and document handling, PaperCut MF requires users to authenticate at the MFD with a variety of login options. Enter a unique ID, username with a correlated password or pin, scan an ID card or badge, or integrate with biometric hardware for the most secure level of identification.

Card numbers can easily be extracted from your network's user directory or a database (e.g. door access control system), or users can self-associate their card on first use.

Watermarking and digital signatures

[Watermarking](#) automatically adds a username, timestamp, digital signature, or other metadata to every printed page. It's a fantastic mechanism to improve behavior in your organization – when users see that printed documents can be traced back to them, it's much less likely they'll let sensitive documents lie around the office.



Secure Print Release

[Secure Print Release](#) increases document security and reduces wasteful, uncollected print jobs. All print jobs sit in a holding state until the user walks up to the multi function device (MFD), logs in, and approves its release. This avoids confidential documents sitting on the paper tray until users can make their way to the MFD, or if a user forgets they pressed "print" at all.



Find-Me Printing

Adding convenience to the already secure mix, [Find-Me Printing](#) saves users from needing to choose what printer they'd like their job sent to. They can print to the shared Find-Me queue, then simply walk up to any printer they like, authenticate, and safely release their job under their strict supervision.

With Find-Me Printing, you'll:

- ▶ Reduce the need for IT administrators to manage multiple print drivers and queues
- ▶ Reduce waste by up to 20% in busy office environments
- ▶ Minimize inconvenience when printers are in error by letting users easily select another

Print archiving

[Print archiving](#) empowers administrators to browse and review the content of print activity in their environment. Alongside the powerful tracking and reporting functionality built into PaperCut MF, this gives administrators a wide range of auditing functions.

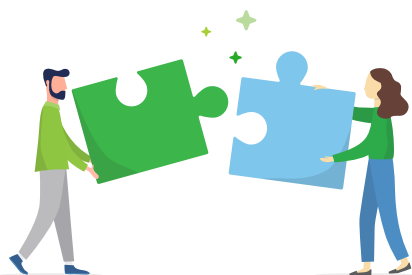
Integrate with third-party systems

System integrations

PaperCut MF has one of the biggest collections of [third-party integrations](#) around, making it as easy as possible to amp up your existing business structure with the added support of PaperCut MF.

You can connect with:

- ▶ Payment gateways
- ▶ Accounting systems
- ▶ Legal practice management software
- ▶ Coworking management software
- ▶ And many more...



Payment gateways

PaperCut MF plays nicely with leading [payment providers](#) – like PayPal, Authorize.Net, RBS WorldPay or CyberSource – to enable real-time, online payments via credit card. It also supports closed or internal payment systems like college fund accounts.

Hardware gateways are available to support a range of cash loaders, self-service kiosks, and bill and coin boxes. For hardware, please reach out to a PaperCut [Authorized Solution Center](#) (ASC).



Manage 3D printing and Print Rooms

3D printing

Managing a [3D print](#) environment? PaperCut MF streamlines the process for everyone. For users, it's enabling them to submit complete job requests and track their progress. For operators? It's giving them the tools to stay on top of orders they need to process, and even communicate with users. It also gets more people using all that great equipment you've invested in!

You're covered for more than 3D printing, too. Services on CNC machines, laser cutters, or any other equipment your lab offers can all be set up. And since it's PaperCut, you can also allocate users' costs to their traditional printing quotas, and run consistent reporting.

Print Rooms

By tracking and managing all activity, PaperCut MF does away with pesky [Print Room](#) problems. No more easily lost email and paper forms, no more charging and quoting across multiple departments, no more frustration.

From when the user submits a job ticket, to when the print room operator reviews, tracks, and completes the project, PaperCut's end-to-end workflow tool keeps things moving along smoothly and efficiently.

You also get the same consistent reporting and cost-allocation convenience available with PaperCut MF.

Give users power

Control at the MFD

Monitor and control all actions directly on your MFD: print, copy, scan, and fax.

With PaperCut MF, users have power at the device to:

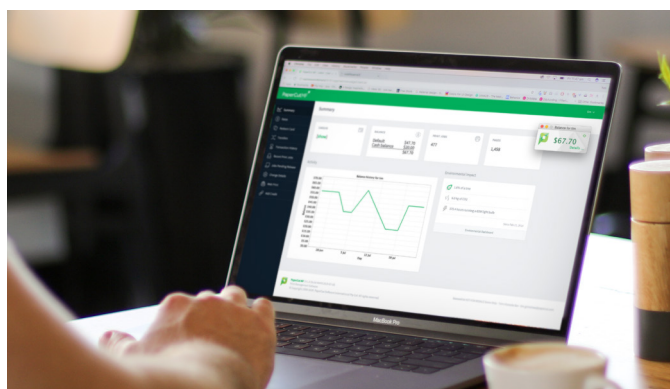
- ▶ Authenticate with username and password, pin, or card swipe
- ▶ Select specific jobs to release or delete
- ▶ Allocate jobs to a personal or shared account
- ▶ Change print settings, including color versus black and white, single-sided versus duplex, or quantity of copies
- ▶ Select scan destinations like email, folder, Google Drive, SharePoint Online, or many more
- ▶ View account balance
- ▶ Select what language the device displays in

And because PaperCut's vendor-neutral, users get that familiar experience on the MFD panel – no matter which printer they go for.



Control from computer, tablet or smartphone

End users have access to a set of web tools to track their activity, check or add to their account balance, and view prior transactions without administrator assistance. Users can even choose from 30 languages when interacting on the PaperCut [web interface](#). Want to brand the users' interface? No problem! Choose custom colors, logos, and messaging to support your organization's spirit.



The [User Client](#) is a pop-up window that allows users to easily view their current account balance, or allocate their print job to a desired personal or shared account. It can also do plenty more to streamline printing and help organizations reduce waste, like:

- ▶ Provide a final notification to confirm what's about to be printed
- ▶ Display system messages like low credit warnings or print policy reminders
- ▶ Show users their impact on the planet - measured in trees, carbon, and energy - with the [environmental widget](#)

Digitize documents

Create smart, searchable documents

With Scan Actions applied, users can convert hard documents into digital masterpieces with just a couple clicks. PaperCut's [Integrated Scanning](#) empowers you to set up scan workflows by user or group, with their settings and scan destinations following them to any compatible MFD in real time.

With [OCR](#) (optical character recognition), you can turn unlimited scans into text-searchable and editable smart documents to retrieve information easier than ever. PaperCut MF's one-click OCR works right out of the box for all kinds of workplaces, and depending on your organization's needs, you can process these intelligent files either in the cloud or locally on site.

Scan to Email and Folders

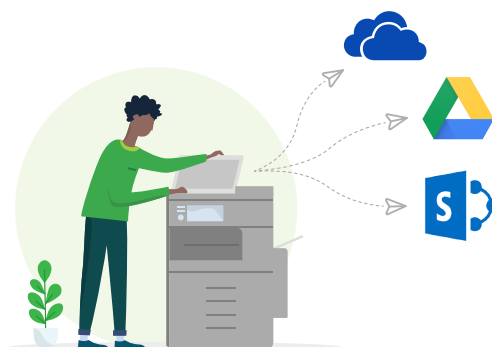
With PaperCut MF, users can quickly scan documents directly to their email account, or to pre-configured personal and network folders with just one click. Files will no longer go to one unorganized "Scanned Documents" folder, causing users to waste time searching for documents.

Scan to Cloud Storage

[Scan to Cloud Storage](#) takes your scans and sends them to the cloud storage service of your choice, like Google Drive, OneDrive, SharePoint Online, Dropbox, and many others. Administrators select which destinations users can access and are able to audit all actions.

But is it secure? Of course! All scan jobs and data are encrypted with signed certificates and transmitted over HTTPS, following industry best practices for security.

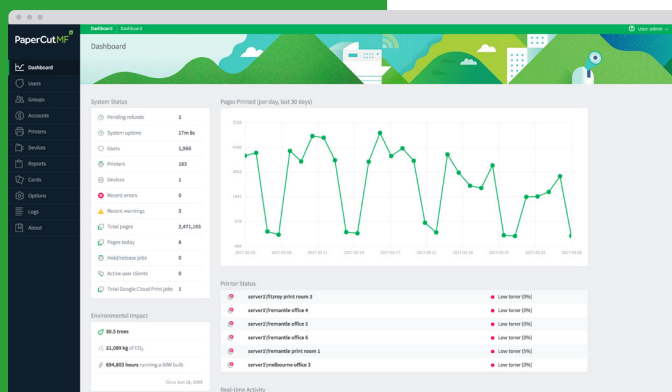
Quick and easy to set up with a one-time authorization, Scan to Cloud Storage requires minimal support and gives users a friendly tap-and-scan workflow. Reducing the extra steps at the MFD means users waste less time.



Get it now

We're all about customers, coding, and coffee. These passions come together to make a product that's powerful yet simple – and we think you'll love it!

Want to try a free 40-day trial, experience a live demo, get a quote, or place an order? Contact a PaperCut Authorized Solution Center (ASC), or email sales@papercut.com for further assistance.



Contact us

sales@papercut.com
papercut.com





A HIGH-LEVEL BENEFIT GUIDE FOR CUSTOMERS

Top 10 reasons to use PaperCut MF

Curious if PaperCut MF is right for you? We've got you covered.

1 It gives your wallet and the environment a welcome break

Reams of paper, boxes of toner, hours of IT support... Waste can really pile up with printing. But with PaperCut MF, you get powerful visibility to see how small choices add up to big impacts. Customizable policies and prompts help users opt for the eco-friendly option; and job attributes can be changed at the printer, showing the positive outcome in real time on the screen.

2 It protects print jobs for your peace of mind

Print systems are complex. Multiple networks and devices are tasked with handling sensitive data constantly open to attack from hackers – inside and out. With PaperCut MF, your data is protected before, during, and after you hit 'print.' Users get validated, jobs stay traceable, and documents can be watermarked to keep costly breaches at bay.

3 It makes releasing print jobs convenient, flexible, and secure

PaperCut's Find-Me Printing solves the needs of IT and users equally. Your IT team manages one secure print queue with any number of printers; and users send jobs to that queue to release at any printer. It's the ultimate tool for document security, as jobs only release when authorized by the sender in person. Plus, if a printer's down, users can simply select another nearby.

4 It lets you print on any device, to any device, from anywhere

Today's users expect to print on demand from any device, which is no mean feat to deliver. PaperCut MF's Mobility Print gets it done with mobile and BYOD (Bring Your Own Device) printing across any brand, model, and operating system. Roaming users? No problem. Print Deploy pushes the right print drivers and queues in bulk to keep on-the-move users printing – even without a server or Active Directory.

5 It makes scanning simple, useful, and future-proof

Recreating PDFs just to edit them, searching for relevant text... Scanning can be frustrating. But with Integrated Scanning and OCR (optical character recognition), users can securely send text-searchable, editable documents to a vast variety of local and cloud-hosted destinations like email, Google Drive, SharePoint, and more – all with a couple of taps on the device.

6 It boasts a variety of flexible syncing and hosting options

Managing user databases isn't exactly a fun pastime. That's why PaperCut MF supports directories of all flavors to keep things hassle-free. Use GoogleSync and Azure AD if you're partial to the cloud; or Active Directory for a more traditional setup. You can even mix and match to make directory transitions that much easier. Better yet, all PaperCut MF data can be hosted on site or in the cloud to meet your needs.

7 It adapts with you and your business in every way

Worried about outgrowing your software? Worry no more. PaperCut MF is highly scalable, flexible, and used by customers with 10s, 100s, or 1000s of printers in the mix. Beyond scaling, PaperCut MF can adapt to any change with support for over 25 printer brands, and commitment to a multi-platform solution. No more hardware decisions held up by software limitations. Rejoice!

8 It surfaces data and insights for meaningful change

Changing behavior without data on current behavior? That's a tough ask. But with PaperCut MF's 75+ built-in reports and custom reporting, you'll get empowering data and insights for all areas – from detailed page logs to summaries by user, department, and device. You can also view, export, print, or schedule email delivery of reports to keep your hands-on involvement low.

9 It's incredibly easy to use for everyone

One of our favorite PaperCut slogans is "it just works." From initial installation and user adaptation, to continued management and implementation of new features, we build software that's easy to use in every way. Plus, our admin console is the most user-friendly and intuitive of any output management platform according to Buyers Lab – so experts and newcomers alike will feel right at home.

10 It's supported by a peerless network of knowledge

Everything we do at PaperCut is centered around our customer-first philosophy – especially when it comes to supporting you at every step. Our 700+ Knowledge Base articles are perfect for self-service DIY fixes, and our global network of support staff and partners means you have access to real people with real answers – in your timezone, on the ground, and often just around the corner.

Take their word for it

68,000 customers across 192 countries managing over 100 million users on 700,000 printers and 2 million Chromebooks. We love it when the global PaperCut family tells the story for us.



"Thanks to PaperCut, **90% of our printer-related issues no longer exist.**"

York Region District School Board



"PaperCut MF is a **huge time saver**. It maintains all of our **print management accounting** and provides **excellent print security.**"

Wall Templeton Attorneys



"Easy to implement, easy to use, easy to support... **It's just so easy.**"

St. Mary's Menston Catholic Academy

QRDOC.IO



v1.0

Scan for new versions
and digital copies

**Contact us to explore more
benefits and features**

sales@papercut.com
papercut.com

PaperCut™

A WHITEPAPER ON PRINT SECURITY

Securing your print system with PaperCut

by PaperCut Software – October 2020





Print security model	5
Securing print infrastructure	5
Securing print workflows	5
Securing printed output	5
Print management	6
Print user authentication	7
Secure connections from end users	7
Print server security	8
Print queues	8
Device security	9
Network	9
Secure connections	9
Physical security	10
Device access	10
Two-factor authentication	11
Firmware	11
Print management solution security	12
Maintaining a secure print system	13
Print policy	14
Secure Print Release	15
Prevent the release of print jobs to a printer in error	15
Job timeout	16
Accountability to the user	16
Print privacy	17
Securing printed output	18
Audit Trails and Reports of printing activity	18



Watermarking and Digital Signatures	19
Electronic archiving of printed documents	20
Authors	24
Contributors	24
PaperCut	24
Support	24



Introduction

Long overlooked by the IT security industry, the importance of printing security is now widely understood. A best-practice information security policy must have a comprehensive set of measures to protect the print system.

This fact is highlighted by the increasing number of printing related security attacks reported in the press. In a 2019 Quocirca report, “more than 66% of companies rank print in their top 5 risks, and 59% reported a print-related data loss in the past year.”¹

Print systems tend to be complex, spanning multiple devices, networks, and operating systems. At the same time, they perform critical business functions and process confidential and sensitive data. These facts lead to a large attack surface that is attractive to hackers and denial of service attackers. As a result, security audits and penetration tests often highlight the print system as the weak point in an organization’s IT security audit. And remember, security attacks and leaks are just as likely to come from inside your organization as outside.

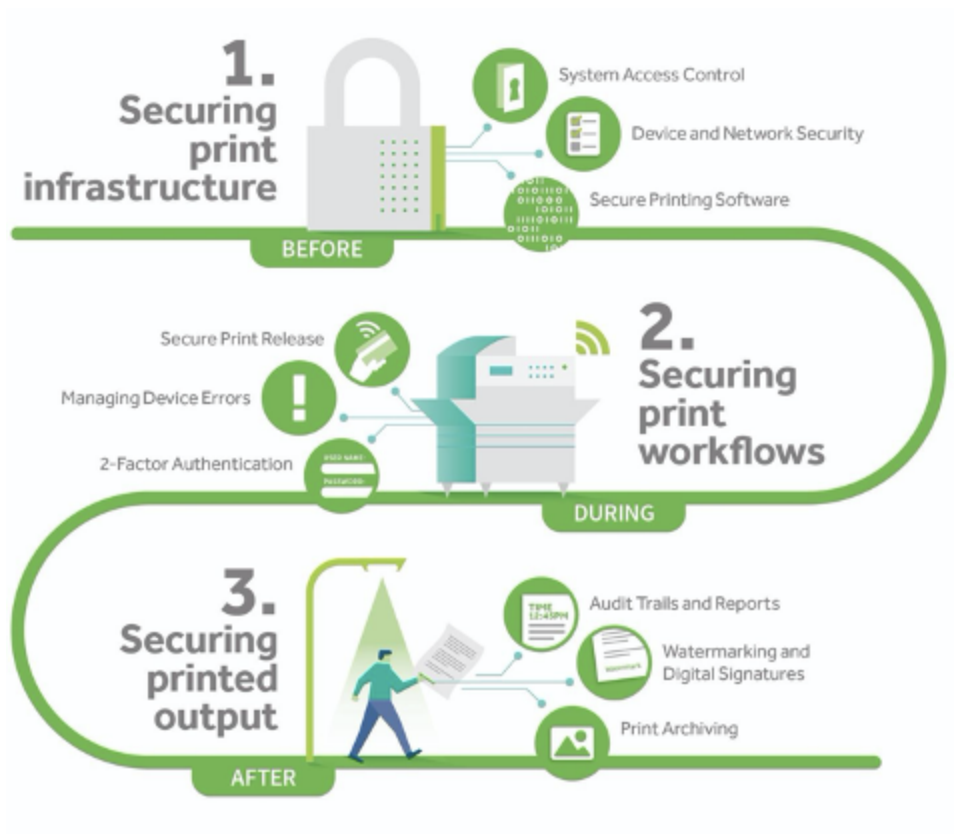
The good news is that effective print security measures are available and well known. As with all good security practices, the approach presented here is multi-layered, covering all parts of the print workflow.



¹ “Global Print Security Landscape” Quocirca 2019



Print security model



Our print security model covers all phases of the printing lifecycle:

Securing print infrastructure

There are many security measures to be taken before a single document is printed. All parts of the print infrastructure should be secured, including workstations, mobile devices, servers, networks, and printers.

Securing print workflows

While your infrastructure may be hardened against attack, your printing workflows might leave you wide open. We recommend some proven and secure print workflows that are straightforward to implement and pay high dividends.



Securing printed output

Once a document is collected from the printer, how do we keep it secure? Several technologies, such as watermarking and print audit logs, work together to allow traceability and encourage correct user behavior.

Print management

Print management software is commonly used to provide many of the traceability and security features described in this whitepaper. For example, secure print release is an important feature of any print management system. Likewise, secure Print Management software is essential for General Data Protection Regulation (GDPR) and Health Insurance Portability and Accountability Act (HIPAA) compliance. GDPR is a major upgrade to data privacy regulations in the EU and is making waves worldwide. If you want to learn more about GDPR, check out our [GDPR Compliance Guide](#).

PaperCut NG or PaperCut MF can support all the security measures described in this document.



Securing print infrastructure

When considering end-to-end print security, it makes sense to start with the infrastructure that supports the printing processes. Think of the network and devices that support the print job from the time a user presses “Print” to creating a printed document.

Print user authentication

Central to many best practices in security (not just print security) is the ability to uniquely and accurately identify the end user. Desktops should require users to authenticate themselves against a centrally managed source of accounts (i.e. Active Directory, eDirectory, LDAP, Open Directory). This way, you can attribute jobs to these users and control access to various devices as needed.

Identifying the user becomes challenging when she chooses to print from their mobile or BYOD device. And a mobile or BYOD device may not require a user to authenticate before access.

Products like PaperCut’s Mobility Print and Print Deploy can bridge this gap by ensuring that jobs are correctly authenticated before being accepted by a print server.

Secure connections from end users

It is becoming much more common for users to be connected to a Zero Trust network, sometimes referred to as BeyondCorp. What this means is that joining the network does not give a user access to anything more than what they would have had access to when connecting to the internet at a coffee shop. It also assumes that the network doesn’t protect users more than what they would have been exposed to on the internet.

PaperCut NG and PaperCut MF helps organizations align their print infrastructure with these goals. Using the Print Deploy feature in PaperCut NG and PaperCut MF, client devices can be restricted to only accept trusted SSL certificates when establishing HTTPS connections. This means that no one on the internet can impersonate the server or intercept any data.

Organizations that prefer to restrict all inbound network traffic to their infrastructure can opt for the Mobility Print Cloud Print feature. With this feature, an encrypted peer-to-peer connection is



established between the client and the server, even if the server only has an outbound internet connection.

Print server security

Most organizations set aside a computer to play the role of the print server, which centralizes printing and makes all the print resources available to end users. It's important to consider the security of this server to ensure its availability and reliability, and to reduce the risk of it being compromised.

From an operating system perspective, updates and patches should be regularly applied to address known vulnerabilities. In addition to regularly updating virus definitions on your print servers, print drivers should be kept up-to-date as part of regular maintenance.

The logical location of the server in the network should also be considered as a way of being able to reduce the attack surface and the threat of attack. Print Servers should be located on the internal network, protected from the internet and DMZ by firewalls. IP addresses on the internal network must not be reachable from an outside network.

Print queues

A commonly overlooked task is to restrict rights to shared print queues. Rights on shared queues should be configured to ensure users aren't able to take control of each other's jobs or change any of the queue settings. For example, a user should not be able to pause a queue or delete another user's job.

It's also worth noting that not all printing protocols require authentication by design. LPR, as an example, will accept print jobs on port 515 from any client, circumventing the normal access rights a server may use. Some scenarios require the use of LPR and in these cases, we recommend you consider adding controls to restrict which clients that can access the LPR port. Another useful hardening strategy is to add secure print release to an LPR queue.

Print encryption can be a useful way to add an additional layer of security to print jobs in process. Starting in PaperCut NG/MF 20.1, print jobs can be encrypted at rest on Windows print servers. Another simple way to implement this is to turn on operating system level encryption on the hard drive used to store print queues. This ensures that backdoor access to the hard drive will not lead to sensitive data leaks.

Not all printers should be accessible to all end users. The Principle of Least Privilege recommends you don't grant any user access to a device (server queue) unless they explicitly need it. For example, you might want to restrict access to a printer that uses paper with the company letterhead to limit the risk of misuse.



Device security

Multifunction Devices (MFDs) and Multifunction Printers (MFPs) are extremely powerful but also vulnerable to misuse and attack. A range of measures are needed to ensure your printer and MFD are hardened against security threats.

Network

MFDs generally need access to your organization's network to perform functions such as user directory lookup (eg. Active Directory), email/send services, and so on. Make sure you use a service account with the correct level of access. Using a user level account can make you vulnerable as they are a hacker's prime target.

In a similar context to securing the print server, the logical network location of the MFDs or MFPs themselves should be considered to reduce their attack surface. Does your printer really need to be accessible from the internet, or even from your Brockway or Ogdenville offices?

Conversely, does your printer need internet access or access to the rest of your internal network? Limiting routability of network traffic from a printer subnet can significantly reduce the impact of an infected rogue device.

We recommend that you use your print server as a gateway to all print devices. Use VLANs or subnetting to ensure that the only device that can see the printers is the print server. This ensures that, as a Systems Administrator, you control access to the device via your server. This can also be achieved using Access Control Lists (ACLs) for account level permissions, or IP filtering for preventing access from specific IP ranges, or other creative means to ensure printers cannot be reached directly.

Secure connections

Where there is an option, devices should be configured to use secure, encrypted network connections (e.g. using HTTPS), especially when sensitive data, such as documents and passwords, are transmitted. While PaperCut NG/MF allows for both HTTP and HTTPS, HTTP Strict Transport Security (HSTS) is available to ensure access is allowed only via an HTTPS connection.

Passwords should never be sent over any network connection in clear text. Configure your network to use the most recent TLS protocols supported by your devices. Certain older protocols, such as SSL and older ciphers such as RC4, have known vulnerabilities and should be disabled.

To avoid man-in-the-middle attacks, TLS connections should ideally require that verified certificates are in place to positively identify the authentication host (such as the host running PaperCut MF). Where a man-in-the-middle attack is assessed as being a low risk, an



automatically generated private cert can be used and the other benefits of TLS, such as encryption are still obtained.

One factor that is becoming increasingly important is knowing your device. MFD manufacturers are offering more and more options for connectivity, such as Bluetooth, Wi-Fi direct, or NFC printing. Of course all of these features are nice, but from a security standpoint, they add to the complexity and risk surface. Make sure you know the capabilities of your devices, and you know what risks you're open to.

Physical security

The physical location of a printer is also as important as the logical network location. Printing productivity can be seriously hampered if printers are constantly exposed to physical damage due to placement in insecure public areas.

Locating printers in places accessible only by authorized users is a simple way to reduce the risk of security breaches.

Campus and school locations can be particularly vulnerable, especially where printers are accessible by the student population. Additional physical security measures that may be taken include:

- Securing the printer to the building, to prevent theft
- Disabling the inbound USB port(s), to prevent direct printing over USB, or direct access to the printer hard drive.
- Protecting the network connection. For example, some sites even use super-glue to secure the network cable in place.
- Locking the paper trays

Device access

Modern MFDs and printers can be thought of as Internet of Things (IoT) servers and are vulnerable to a range of IoT attacks. All modern devices are shipped with a rich set of protocols and services, most of which may never be used by your organization. To reduce the surface area of attack, we recommend turning off any unused device protocols and services.

Ensure default administrator passwords are periodically changed and use secure passwords for machine settings, such as IP address, to prevent alteration by users or malicious code on the network. Often, factory default passwords are well known to hackers, leaving devices highly vulnerable to attack.



Many devices allow print jobs to be stored on an internal hard disk or internal memory for re-printing. If this feature is used, clear policies are needed to ensure that only public documents are stored, or that documents are adequately password protected. In many cases, it may be prudent to disable this feature. Alternatively, if you do not want to store jobs for reuse, most MFDs provide a data overwrite feature. This allows print data to be overwritten or removed, either immediately, on demand, or at scheduled intervals.

Many modern MFDs have a feature to encrypt all partitions of the hard drive that might contain customer data with Advanced Encryption Standard (AES) encryption. You should ensure this feature is enabled.

Some MFD manufacturers bundle these features (print job deletion, data overwrites and data encryption) into Data Security Kits which may be optionally purchased. If you need these features, you must ensure the appropriate Data Security Kit is purchased and installed.

Two-factor authentication

MFDs and some printers provide for user authentication at the device through card swipe, ID number or other methods. This is an important safeguard to prevent unauthorized access to a device.

Two-factor authentication provides an additional layer of security by requesting a user for additional authentication information. PaperCut MF, for example, provides for a PIN to be entered as the second factor to authenticate a user after swiping their card or entering their ID number.

Firmware

Printer manufacturers are becoming increasingly conscious of security and are actively updating their firmware to address security issues reported against their devices. A practice of regularly updating device firmware is needed to ensure you benefit from any security fixes from the manufacturers.

The cryptographic technology on MFDs varies and sometimes lags behind current best practice. However the industry is becoming more security aware and keeping your MFD firmware up-to-date is important to ensure your MFDs use the most up-to-date ciphers available for the device.

Older ciphers, such as RC4, are susceptible to security breaches. By default, PaperCut MF is configured to support a wide variety of TLS ciphers for compatibility purposes. PaperCut is bundled with a recent version of the Java SE Runtime Environment, which incorporates the latest security fixes. When PaperCut connects to a device, the two communicate and pick the most secure cipher that is mutually supported.



Print management solution security

Regardless of which product you choose to account for or control your printing (naturally, we recommend PaperCut NG or PaperCut MF), there are some considerations and recommendations we would make here as well.

Sensitive information should be secure while being transmitted between the application components. Check for protocols such as HTTPS being supported when accessing administration interfaces and between embedded applications and servers.

Data that is stored, is also an important consideration. Are you free to use and secure a database of your choice and manage backups to your organization's standards?

PaperCut NG and PaperCut MF were developed from the ground-up with security in mind. With a strong heritage in the education market, the software has been battle-tested and security-hardened over years of student attacks at schools and universities around the world.

PaperCut retains a strong security culture, with both proactive and reactive security practices built into our company's processes. We regularly review third party components for security vulnerabilities. All incoming security reports are immediately reviewed by our PaperCut Security team. Any mitigating or defensive workarounds are put in place and fixes implemented and published typically within days.

We respectfully recommend you look for strong security credentials with any print software you introduce into your workflow.

Specific security hardening measures used by PaperCut NG/MF and other security minded solutions include:

- Process isolation — print management software should run in isolated processes away from the operating system kernel. Processes should run under the minimum necessary user privileges. For example, it should not be necessary to run long- running tasks under the root or administrator user.
- Secured APIs — public APIs should have multiple layers of security. PaperCut uses authentication tokens coupled with IP address filtering to ensure that API calls are properly authenticated and are from a trusted source.
- Code signing — your installers and code should be code-signed by the vendor to give assurances that you are running unmodified code that is authored directly by the vendor.
- Sandboxing — when there's even a small risk that aspects of the solution could become compromised, we work to engineer the solution to anticipate the threat and contain any damage. Sandboxing is one method where VMs, or process-level isolation techniques, are



used to add layers into the system so that a compromise in one area/ component does not open up a whole system.

- Secure web pages — web pages should have built-in protections against SQL injection, Cross-Site forgery and Cross-Site Scripting attacks.
- Directory Services — (such as Google, AD, LDAP, etc) should be leveraged to authenticate users in preference to storing passwords in the print management system. If users are defined outside a directory service (e.g. guest printing accounts), the password should be securely encrypted. PaperCut NG/MF uses Bcrypt for this purpose.
- Fail-Closed Design — an important security principle is to shut down access, such as the network connection from an MFD to the authentication server, whenever a failure occurs. With a “fail-open design”, a simple action like removing a network cable, could render a device open to attack. PaperCut NG/ MF uses a “fail- closed design” as a core design principle in all print security areas.
- General Data Protection Regulation (GDPR) compliance—GDPR is a major upgrade to data privacy regulations in the EU and is making waves worldwide. GDPR gives control of personal data back to the individual, and generally improves data privacy with a uniform set of regulations. If you want to learn more about GDPR, check out our GDPR Compliance Guide.

Maintaining a secure print system

It is important to recognize the business critical nature of your print infrastructure and apply standard IT best practices to your print systems, including your print management system. Some examples of best practices include:

- Regular security audits to ensure vulnerabilities to print exploits have not crept in.
- Regular backups of print management databases.
- Maintenance and patching of your print management software.
- A tested Disaster Recovery Plan.



Securing print workflows

While your infrastructure may be hardened against attack, your printing workflows may leave you wide open. We present a range of secure print workflows that are easy to implement and highly effective.

Print policy

What are the right print policies for your organization? Should print jobs printed out of normal business hours be allowed? Should certain users have restricted printing permissions? Once you have a clear idea of the policies you need to implement, you can then focus on implementing these policies and business rules.

North Shore High School would like to allow their students to print some documents for free, but only during class time, and only selected documents. The best way to implement this is for teachers to approve (or deny) all student printing. Using PaperCut NG/MFs print policies, North Shore High School can enforce the use of a teacher's approval code for all student print jobs.

Implementing business printing policies can take many forms. Printing out key policies and distributing them prominently across your organization can be a useful exercise, but does not guarantee that all employees and guests will follow this guidance. An application like PaperCut NG/MF allows an organization to implement these print policies and business rules automatically, via built-in and customizable recipes.

Print policy example

North Shore High School would like to allow their students to print some documents for free, but only during class time, and only selected documents. The best way to implement this is for teachers to approve (or deny) all student printing. Using PaperCut NG/MF's print policies, North Shore High School can enforce the use of a teacher's approval code for all student print jobs.



Secure Print Release

In a standard printing environment, print jobs are sent directly to the printer for immediate printing. A large proportion of these jobs are typically not required and end up left on the printer or put in the waste bin. Any jobs not collected immediately are a security risk, if the documents are sensitive or confidential.

Secure Print Release is a simple solution that places jobs in a holding state until the user authenticates and releases the job at the printer. Users should be able to either manually select jobs to release or have jobs automatically print after successful authentication. Sensitive jobs will then not sit uncollected at the printer!

Secure Print Release, sometimes also called mailbox printing, is an important feature to consider when designing your print workflow. This feature allows the user who printed the document to release the document only when they are physically located in front of the MFD or printer. Most MFDs support this functionality. However, to achieve a consistent user experience across your fleet of devices, a print management solution, such as PaperCut NG or PaperCut MF, is recommended.

PaperCut NG and PaperCut MF also offer Find-Me printing. Find-Me printing provides a roaming print solution where users print to a single queue. All print jobs are then “pulled” to the specific printer at which a user identifies herself, e.g. by swiping an access card.

Secure Print Release example

Stephanie White from White & Turner Legal Services has sent a confidential contract to a printer. After she has sent the document, a colleague stops by for a chat so she cannot get to the printer straight away. With Secure Print Release, she is not concerned as she knows the document will not be printed until she releases the document at the printer.

Prevent the release of print jobs to a printer in error

Secure Print Release is an essential capability of a secure printing environment. But what happens when jobs are released to a printer that is in an error state? For example, a printer that has a paper jam or is out of toner? What would happen if the printer error got resolved, and these jobs started printing automatically in the absence of the authorized user?



These jobs should not print automatically when the printer error is resolved after the user has walked away.

PaperCut NG/MF offers the ability to prevent the release of jobs when a printer is in error. When the printer error is resolved, the user must then re-release the job, thus giving control back to the user about when their job prints and eliminating the possibility of sensitive data being leaked.

Printer in error example

Stephanie White from White & Turner Legal Services is now at the printer and has released her print job. However, while the job before hers is being printed, the toner runs out. She contacts her assistant about changing the toner, but doesn't have time to hang around and wait. After about an hour, she goes back to the printer to try to re-release her job, but much to her dismay, the document has already been printed and has been sitting on the printer since the low toner error was corrected. A secure print management system can avoid this by preventing the release of jobs to a printer in error.

Job timeout

Print output left sitting in a printer tray is not the only way sensitive print data can be accessed by someone other than the owner. Spool files stored on the print server waiting to be released may also be viewed if accessed by malicious individuals. While the measures outlined in the “Securing the Print Infrastructure” section can help protect against this, jobs should be automatically removed from the hold release print queue after an appropriate period of time. This also allows you to reduce the load on your print server and save paper and toner by eliminating printing of jobs that are no longer needed.

PaperCut NG/MF allows you to define how long a print job stays in this hold release print queue before it is automatically deleted.

Accountability to the user

There is nothing like knowing that what you print can be tracked and audited to prevent people from printing their favorite thesis on whether Captain Kirk or Captain Picard is the better captain in Star Trek, including all 55 full color pages of the Starship Enterprise schematics!



While this capability is available through operating system audits (e.g. Windows event viewer), it can be a manual, time-consuming and error-prone process. PaperCut NG/MF allows you to centrally manage this process for all devices and users.

PaperCut NG/MF allows you to share some or all of a user's printing history with them in several ways. You can simply share their print history with them or you can quota their printing ability and have them initiate a request and justification for more printing once they hit their limit.

Print privacy

Gossips are relentless. The last thing you want is to have weeks of secretive work all undone because the document titled "Surprise Employee Bonuses.docx" is seen sitting in a print queue, waiting to be printed! Where possible, you should hide your sensitive data.

While you could solve this via a complex LPD/LPR setup, PaperCut NG/MF allows you to hide the document names either at an individual print queue level or across your entire print server. Your employee surprise bonuses will remain a surprise now!



Securing printed output

Keeping information secure is never easy, but it gets a whole lot harder once in printed form! All's not lost, however, as there are several technologies and best practices available that can significantly improve the traceability and security of printed documents and prevent document theft.

As users are in control of printed documents, security measures for printed documents must effectively drive user behavior. For example, a policy document sitting in a drawer is unlikely to prevent a private medical record being left behind in the hospital cafe. But if the medical record contained a prominent digital signature that could easily trace the document owner, more care would be taken by that person before printing the material and abandoning it at a public place.

Document security best practice is to use a range of complementary measures, which include:

- Audit trails and reports of printing activity
- Watermarking and digital signatures
- Electronic archiving of printed documents

Audit Trails and Reports of printing activity

A secured print system should keep a comprehensive record of all user print jobs. This should include information identifying the user who printed the document, the document name, the computer used to generate the print job, the output device, and the date and time of printing.

The existence of this audit trail enhances accountability and traceability, and encourages users to act with integrity.

PaperCut NG/MF retains detailed information in logs and archives. In addition, PaperCut NG/MF offers a wide range of audit reports detailing all transactions that have occurred in the system.

System activity

PaperCut retains detailed system level information in the following logs:



- Audit logs — all operations against user accounts are recorded in an audit log. These audit records capture the date, details, and the user who performed the operation.
- Application log — PaperCut NG/MF retains a complete history of system events including, errors, notifications, alerts, new printers or devices, etc.

User activity

At the user level, PaperCut NG/MF provides the following logs to track user activity:

- Job log — a log of all the print, copy, fax, and scan jobs, capturing information about the user, date, and details for each job.
- Transaction log — a record of all the financial transactions, including print job charges and account balance transactions.

Reporting

Regular, scheduled reports can be used to alert administrators of unusual printing behavior or contravene an organization's printing policies.

PaperCut NG/MF offers a wide range of comprehensive reports that can be generated on demand or automatically emailed to management on a daily, weekly or monthly schedule.

Watermarking and Digital Signatures

Watermarking is a technology that augments a printed page with text added at the time of print. A watermark may contain information such as the user who printed the document, the date on which it was printed, and the printer used. In this way, watermarking can act as a reminder to users that the source of a document can be identified and traced back to them.



A digital signature is a digital code uniquely generated by taking various print job attributes, such as print time, username, printer name, and document name, and combining them with a secret key. A digital signature applied to a printed document as a watermark can be used to quickly trace a printed document back to a specific entry in the print audit log.



Best practice printed document security combines these three features — watermarking, digital signatures, and a comprehensive print log — to provide full traceability and security of printed documents.

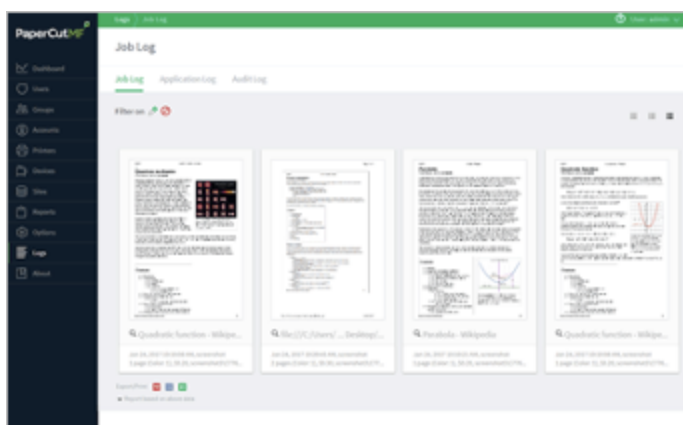
PaperCut NG/MF enhances document security by providing all three features, working in tandem — watermarking, digital signatures, and a comprehensive print log searchable by digital signature.

Watermarking example

Damien Turner from White & Turner Legal Services has been working on a high profile divorce case, but much to his horror, has discovered that details of the proposed settlement have been leaked to the press. The magazine in question has provided the source document and because White & Turner Legal Services use PaperCut's digital signature watermarking functionality, which automatically prints a secret key on all documents, Damien is able to identify when and where the document was printed and more importantly, who was responsible.

Electronic archiving of printed documents

Observing document retention requirements, e.g. HIPAA compliance, is a huge burden on many companies. Maintaining printed archives is both expensive and time-consuming. Automatic electronic archiving of all printed documents is an attractive solution.



The ability to electronically archive printed documents also adds another layer of print output security. With electronic archiving, the print log is augmented by an image of the printed document, allowing for complete traceability. For example, an archive can positively identify



who printed an incriminating or offensive document, since the print logs includes the contents of the print output.

PaperCut NG/MF's Print Archiving empowers approved administrators to browse and review the content of print activity within their environment. Alongside the powerful tracking and reporting functionality built into PaperCut NG/MF, this gives system administrators a wide range of auditing capabilities, such as:

Storing historic records of all printed content.

- Viewing past print jobs in a web browser.
- Having fined-grained access control to archived content.
- Downloading the original spool file for reprinting with 100% fidelity.
- Enabling or disabling archiving for selected printers and users.

Archiving example

When Stephanie was at the printer, she noticed another print out of a rather offensive image, but had no idea who had printed it. With electronic archiving, the System Administrator can track down the culprit. The SysAdmin can view an image of every print job to identify the one in question, and once the job is identified, can see who was responsible for printing offensive material in the workplace.



Summary

Practical and proven methods are available to secure your print system. We recommend a multi-layered security strategy that addresses vulnerabilities before, during, and after each document is printed.

Securing your print infrastructure, through defensive network configuration, secure print queues and protecting device access will help ensure you have a robust print system even before the first job is printed.

Securing your print workflows through print policy, secure print release, and managing jobs released to a printer in error, are effective and widely used tools with the out-of-box solutions readily available.

Securing your print output using a combination of print audit logs, watermarking with digital signatures and electronic archiving, will help drive correct user behavior and force accountability for printed documents.

A comprehensive print management solution, such as PaperCut NG and PaperCut MF will help organizations implement many of these best practices in a cost-effective way to achieve a secure print system. Of course, the print management software must have its own strong security credentials.

Additional up-to-date information may be obtained from PaperCut's web site at:

<http://www.papercut.com/kb/Main/Security>

Please contact PaperCut support or your local PaperCut reseller if you have specific questions not addressed by this white paper or the online documentation.



Print security checklist

Use this checklist to assess the health of your print system security

1. Securing print infrastructure + Is there secure network communication between the end user and the MFD? + Have you separated the print server from the network to protect traffic from interception? + Are you monitoring and investigating any packet sniffing or port scanning behavior on the network? + What happens to your print data during network outages? + Are you hiding document names in your print queues? + Have you disabled the USB ports on MFDs to prevent someone from scanning to USB devices? + Has all unused MFD functionality been disabled? + Have you applied all patch updates and do you have a security patch update procedure that tackles the latest vulnerabilities as they happen? + Is there any sensitive network information stored in your MFDs? Are device passwords (such as the admin password) updated and secure? + What happens to your devices at the end of their life? Does the hard drive and internal memory of every printer get erased and securely disposed of at the end of its life? + Are you adhering to industry standards, such as specifications established by the US Department of Defense (DoD)? + Has your organization invested in any Data Loss Prevention (DLP) technology? If yes, how is this complemented or compromised by your print security? + Are the same print security settings employed consistently across all devices from desktop PCs, to tablets and smartphones? + Are your MFDs secured or located in a position where CCTV cameras or people can view them so that malicious activity can be both detected and deterred?	2. Securing print workflows + Can anyone (even a visitor) walk up to your MFDs and copy, scan, or fax any document? + Can they scan any document to a folder, email, or fax? + Are printed jobs left unattended in the output trays of printers and copiers? + Can users bypass the system and print directly from a print server or a local queue on their computer to the IP address of a printer? + How are you encouraging and enforcing your print policies? + Are you enforcing a secure print release policy? + Have you enabled print job timeout for older documents on your print server?
	3. Securing print output + Do you maintain an audit trail of print, copy, scan, and fax activity? That is: who, what, when, where, and how? + When archiving documents, are you using a file format that allows for long-term preservation? + Do you use watermark technology to help classify sensitive documents and highlight what is vulnerable? Do you use digital signatures to identify who printed a document? + Have all end users been adequately trained, not only in how to use a print system, but also on what your organization's print policies are, and the impacts of policy breaches to your organization?



Thank you

Authors

Chris Dance (CEO, PaperCut Software)

Geoff Smith (Head of Development, PaperCut Software)

Anthony Nicola (Head of Support, PaperCut Software)

Damien White (Global Technical Services Manager, PaperCut Software)

Contributors

Mark Hart (ACDI – Director of Business Development / National Accounts)

PaperCut

sales@papercut.com

papercut.com

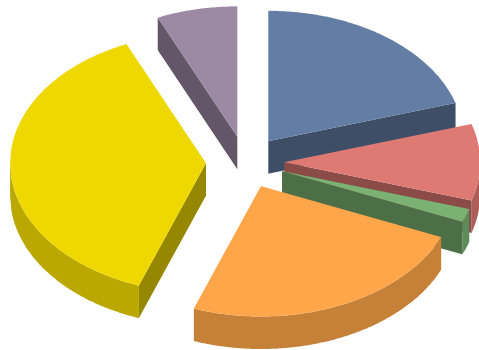
Support

support@papercut.com

papercut.com/support

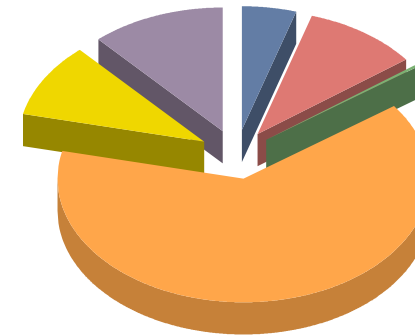
City of Decatur

Volume by Equipment Type



Desktop - Color MFP	4,015	20.2%
Printer - B & W Laser	1,916	9.6%
Printer - B & W Laser	333	1.7%
Printer - Color Laser	4,767	24.0%
Printer - Color Laser	7,551	38.0%
Printer - Inkjet	1,305	6.6%
Total:	19,887	100.0%

Cost by Equipment Type



Desktop - Color MFP	\$95	4.7%
Printer - B & W Laser	\$198	9.9%
Printer - B & W Laser	\$10	0.5%
Printer - Color Laser	\$1,280	63.7%
Printer - Color Laser	\$191	9.5%
Printer - Inkjet	\$237	11.8%
Total:	\$2,012	100.0%



City of Decatur

Desktop - Color MFP

Model	Department	Location	Serial #	Age	Black Volume	Color Volume	Mono CPP	Color CPP	Mono TCO	Color TCO
HP Color LaserJet MFP M577			MXCCL46037	0.0	720	625	0.01036	0.03194	\$7.46	\$19.96
HP Color LaserJet MFP M577			MXCCL7209L	0.0	800	620	0.01036	0.03194	\$8.29	\$19.80
HP LaserJet 500 color MFP M575			MXCCF441NW	0.0	739	511	0.01718	0.05297	\$12.70	\$27.07
Total Units	3	Equipment Type Sub Total		0.0	2,259	1,756	0.01259	0.03806	\$28.45	\$66.83

Printer - B & W Laser

Model	Department	Location	Serial #	Age	Black Volume	Color Volume	Mono CPP	Color CPP	Mono TCO	Color TCO
hp LaserJet 4250			CNGXD50529	0.0	769	0	0.06476	0.00000	\$49.80	\$0.00
HP LaserJet M402dn			PHB5B57595	0.0	607	0	0.12800	0.00000	\$77.70	\$0.00
HP LaserJet P2015 Series			CNBJS33174	0.0	59	0	0.11555	0.00000	\$6.82	\$0.00
HP LaserJet P2035n			VNB3K03396	0.0	481	0	0.13325	0.00000	\$64.09	\$0.00
Total Units	4	Equipment Type Sub Total		0.0	1,916	0	0.10355	0.00000	\$198.41	\$0.00



City of Decatur

Printer – B & W Laser

Model	Department	Location	Serial #	Age	Black Volume	Color Volume	Mono CPP	Color CPP	Mono TCO	Color TCO
HP LaserJet Pro M148dw			VNB4M00623	0.0	333	0	0.02995	0.00000	\$9.97	\$0.00
Total Units	1		Equipment Type Sub Total	0.0	333	0	0.02994	0.00000	\$9.97	\$0.00



City of Decatur

Printer - Color Laser

Model	Department	Location	Serial #	Age	Black Volume	Color Volume	Mono CPP	Color CPP	Mono TCO	Color TCO
HP Color LaserJet CP2025dn			CNGS301454	0.0	0	0	0.00000	0.00000	\$0.00	\$0.00
HP Color LaserJet MFP M281fdw			VNBNL4DBYP	0.0	18	102	0.14837	0.54068	\$2.67	\$55.15
HP Color LaserJet MFP M476dn			CNB8GBBF6M	0.0	3	3	0.13175	0.45842	\$0.40	\$1.38
HP Color LaserJet MFP M477fdw			VNBKL3PC0H	0.0	0	0	0.00000	0.00000	\$0.00	\$0.00
HP Color LaserJet Pro Mfp M479fdw			MXBCMB60Q7	0.0	0	333	0.00000	0.47697	\$0.00	\$158.83
HP LaserJet 300 colorMFP M375nw			CNC8F1F085	0.0	949	695	0.13166	0.46241	\$124.94	\$321.37
HP LaserJet 300 colorMFP M375nw			CNC8F1H9CY	0.0	424	0	0.13166	0.33075	\$55.82	\$0.00
HP LaserJet 400 color M451dn			CNDF292328	0.0	735	605	0.13166	0.46241	\$96.77	\$279.76
HP LaserJet 400 colorMFP M475dn			CNC8DBLSCX	0.0	3	5	0.13166	0.46241	\$0.39	\$2.31
HP LaserJet 400 colorMFP M475dn			CND8F3F6NW	0.0	34	0	0.13166	0.33075	\$4.48	\$0.00
HP LaserJet 400 colorMFP M475dn			CND8F767L1	0.0	325	89	0.13166	0.46241	\$42.79	\$41.15
HP OfficeJet Pro 9010 series			TH93I3829V	0.0	72	372	0.07677	0.23286	\$5.53	\$86.63
Total Units	12		Equipment Type Sub Total	0.0	2,563	2,204	0.13023	0.42948	\$333.79	\$946.58



City of Decatur

Printer – Color Laser

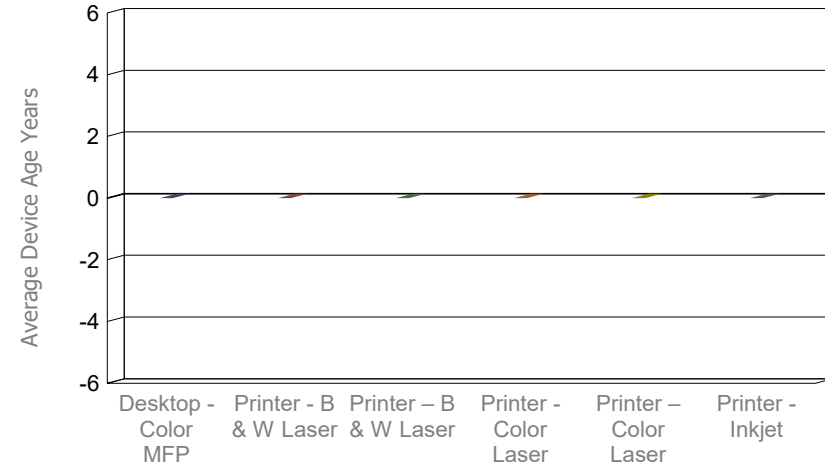
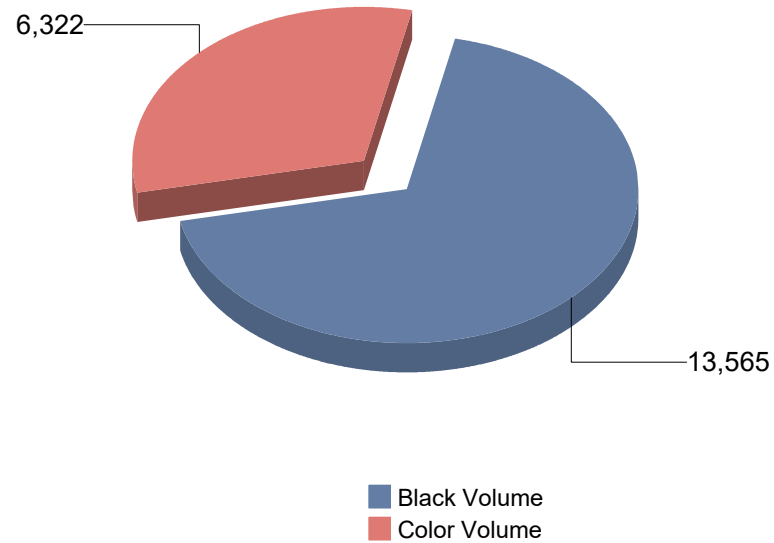
Model	Department	Location	Serial #	Age	Black Volume	Color Volume	Mono CPP	Color CPP	Mono TCO	Color TCO
HP Color LaserJet M652			JPBCK5R0YC	0.0	2,809	537	0.01745	0.05380	\$49.01	\$28.89
HP LaserJet 500 color M551			CNCCF52022	0.0	3,072	1,133	0.01718	0.05297	\$52.78	\$60.02
Total Units 2		Equipment Type Sub Total		0.0	5,881	1,670	0.01731	0.05324	\$101.79	\$88.91

Printer - Inkjet

Model	Department	Location	Serial #	Age	Black Volume	Color Volume	Mono CPP	Color CPP	Mono TCO	Color TCO
HP Officejet Pro 276dw MFP			CN554CV1B6	0.0	3	102	0.09108	0.28651	\$0.27	\$29.22
HP Officejet Pro 276dw MFP			CN584DV055	0.0	225	185	0.09108	0.28651	\$20.49	\$53.00
HP OfficeJet Pro 8710			CN6APH31M6	0.0	248	113	0.08151	0.25287	\$20.21	\$28.57
HP OfficeJet Pro 8710			CN6ATHW2T2	0.0	1	233	0.08151	0.25287	\$0.08	\$58.92
HP OfficeJet Pro 8710			CN7C1BW02J	0.0	0	0	0.00000	0.00000	\$0.00	\$0.00
HP OfficeJet Pro 8710			CN7C2BW0K0	0.0	136	59	0.08151	0.25287	\$11.09	\$14.92
Total Units 6		Equipment Type Sub Total		0.0	613	692	0.08506	0.26681	\$52.14	\$184.63

City of Decatur

Grand Totals



	Total Units	Age	Black Volume	Color Volume	Mono CPP	Color CPP	Mono TCO	Color TCO	Grand Total for All TCO
Grand Totals	28	0.00	13,565	6,322	0.05341	0.20357	\$724.55	\$1,286.95	\$2,011.50

RFP 22-124 (Managed Print Services)

EDGE Business Systems

Print Fleet and Monthly Usage Patterns

Department	Facility	Facility Address	Machine Type	Serial Number	Meter Type	Monthly Volume Snapshot	Cost Per Page	Monthly Usage Cost
Recreation, Parks & Cultural Services	Arts Center	238 Canton St, Alpharetta, GA 30009	AltaLink C8035	3TX396961	B\W	576	\$0.0139	\$8.01
Recreation, Parks & Cultural Services	Arts Center	238 Canton St, Alpharetta, GA 30009	AltaLink C8035	3TX396961	Color	832	\$0.0700	\$58.24
City Administration	City Hall	2 Park Plaza, Alpharetta GA 30009	AltaLink C8045	8TB604952	B\W	873	\$0.0135	\$11.79
City Administration	City Hall	2 Park Plaza, Alpharetta GA 30009	AltaLink C8045	8TB604952	Color	3,152	\$0.0700	\$220.64
Recreation, Parks & Cultural Services	Wills Park Recreation Center	11925 Wills Rd, Alpharetta, GA 30009	AltaLink C8045	8TB603958	B\W	965	\$0.0135	\$13.03
Recreation, Parks & Cultural Services	Wills Park Recreation Center	11925 Wills Rd, Alpharetta, GA 30009	AltaLink C8045	8TB603958	Color	294	\$0.0700	\$20.58
Recreation, Parks & Cultural Services	Adult Activity Center	13450 Cogburn Rd, Milton, GA 30004	AltaLink C8055	8TB600778	B\W	1,178	\$0.0135	\$15.90
Recreation, Parks & Cultural Services	Adult Activity Center	13450 Cogburn Rd, Milton, GA 30004	AltaLink C8055	8TB600778	Color	666	\$0.0700	\$46.62
Community & Economic Development	City Hall	2 Park Plaza, Alpharetta GA 30009	AltaLink C8070	6TB447421	B\W	3,274	\$0.0135	\$44.20
Community & Economic Development	City Hall	2 Park Plaza, Alpharetta GA 30009	AltaLink C8070	6TB447421	Color	2,768	\$0.0700	\$193.76
Finance	City Hall	2 Park Plaza, Alpharetta GA 30009	AltaLink C8070	6TB447291	B\W	4,140	\$0.0135	\$55.89
Finance	City Hall	2 Park Plaza, Alpharetta GA 30009	AltaLink C8070	6TB447291	Color	2,275	\$0.0700	\$159.25
Court	Municipal Court	13690 Highway 9 (Building B), Milton, GA 30004	AltaLink C8135	ELQ514699	B\W	2,806	\$0.0135	\$37.88
Court	Municipal Court	13690 Highway 9 (Building B), Milton, GA 30004	AltaLink C8135	ELQ514699	Color	1,234	\$0.0700	\$86.38
Recreation, Parks & Cultural Services	Equestrian Center	11915 Wills Rd, Alpharetta, GA 30009	ColorQube 8570/DNM	XFN138476	B\W	200	\$0.0135	\$2.70
Recreation, Parks & Cultural Services	Equestrian Center	11915 Wills Rd, Alpharetta, GA 30009	ColorQube 8570/DNM	XFN138476	Color	150	\$0.0700	\$10.50
Public Safety	Public Safety Headquarters	2565 Old Milton Pkwy, Alpharetta, GA 30009	Phaser 6022	PSA069246	B\W	200	\$0.0135	\$2.70
Public Safety	Public Safety Headquarters	2565 Old Milton Pkwy, Alpharetta, GA 30009	Phaser 6022	PSA069246	Color	150	\$0.0700	\$10.50
Court	Municipal Court	13690 Highway 9 (Building B), Milton, GA 30004	VersaLink C400	7HB471184	B\W	200	\$0.0135	\$2.70
Court	Municipal Court	13690 Highway 9 (Building B), Milton, GA 30004	VersaLink C400	7HB471184	Color	504	\$0.0700	\$35.28
Finance	City Hall	2 Park Plaza, Alpharetta GA 30009	VersaLink C400	7HB946305	B\W	583	\$0.0135	\$7.87
Finance	City Hall	2 Park Plaza, Alpharetta GA 30009	VersaLink C400	7HB946305	Color	249	\$0.0700	\$17.43
Public Safety	Public Safety Headquarters	2565 Old Milton Pkwy, Alpharetta, GA 30009	VersaLink C400	7HB780689	B\W	200	\$0.0135	\$2.70
Public Safety	Public Safety Headquarters	2565 Old Milton Pkwy, Alpharetta, GA 30009	VersaLink C400	7HB780689	Color	150	\$0.0700	\$10.50
Finance	City Hall	2 Park Plaza, Alpharetta GA 30009	VersaLink C405	4HX593106	B\W	200	\$0.0135	\$2.70
Finance	City Hall	2 Park Plaza, Alpharetta GA 30009	VersaLink C405	4HX593106	Color	150	\$0.0700	\$10.50
Finance	City Hall	2 Park Plaza, Alpharetta GA 30009	VersaLink C405	4HX593136	B\W	200	\$0.0135	\$2.70
Finance	City Hall	2 Park Plaza, Alpharetta GA 30009	VersaLink C405	4HX593136	Color	150	\$0.0700	\$10.50
Finance	City Hall	2 Park Plaza, Alpharetta GA 30009	VersaLink C405	4HX593142	B\W	200	\$0.0135	\$2.70
Finance	City Hall	2 Park Plaza, Alpharetta GA 30009	VersaLink C405	4HX593142	Color	150	\$0.0700	\$10.50
Finance	City Hall	2 Park Plaza, Alpharetta GA 30009	VersaLink C405	4HX813858	B\W	1,436	\$0.0135	\$19.39
Human Resources	City Hall	2 Park Plaza, Alpharetta GA 30009	VersaLink C405	4HX813858	Color	718	\$0.0700	\$50.26
Public Safety	Public Safety Headquarters	2565 Old Milton Pkwy, Alpharetta, GA 30009	VersaLink C405	4HX593107	B\W	2,438	\$0.0135	\$32.91
Public Safety	Public Safety Headquarters	2565 Old Milton Pkwy, Alpharetta, GA 30009	VersaLink C405	4HX593107	Color	124	\$0.0700	\$8.68
Public Safety	Public Safety Headquarters	2565 Old Milton Pkwy, Alpharetta, GA 30009	VersaLink C405	4HX805542	B\W	254	\$0.0135	\$3.43
Public Safety	Public Safety Headquarters	2565 Old Milton Pkwy, Alpharetta, GA 30009	VersaLink C405	4HX805542	Color	150	\$0.0700	\$10.50
Public Works	Public Works Headquarters	1790 Hembree Rd, Alpharetta, GA 30009	VersaLink C405	4HX593297	B\W	200	\$0.0135	\$2.70
Public Works	Public Works Headquarters	1790 Hembree Rd, Alpharetta, GA 30009	VersaLink C405	4HX593297	Color	150	\$0.0700	\$10.50
Recreation, Parks & Cultural Services	Wills Park Pool	1815 Old Milton Pkwy, Alpharetta, GA 30009	VersaLink C405	4HX800561	B\W	554	\$0.0135	\$7.48
Recreation, Parks & Cultural Services	Wills Park Pool	1815 Old Milton Pkwy, Alpharetta, GA 30009	VersaLink C405	4HX800561	Color	150	\$0.0700	\$10.50
Recreation, Parks & Cultural Services	City Hall	2 Park Plaza, Alpharetta GA 30009	VersaLink C405	4HX816573	B\W	1,113	\$0.0135	\$15.03
Recreation, Parks & Cultural Services	City Hall	2 Park Plaza, Alpharetta GA 30009	VersaLink C405	4HX816573	Color	326	\$0.0700	\$22.82
Public Safety	Public Safety Headquarters	2565 Old Milton Pkwy, Alpharetta, GA 30009	VersaLink C505	3RB728688	B\W	154	\$0.0135	\$2.08
Public Safety	Public Safety Headquarters	2565 Old Milton Pkwy, Alpharetta, GA 30009	VersaLink C505	3RB728688	Color	319	\$0.0700	\$22.33
Public Safety	Public Safety Headquarters	2565 Old Milton Pkwy, Alpharetta, GA 30009	VersaLink C505	3RB731582	B\W	250	\$0.0135	\$3.38
Public Safety	Public Safety Headquarters	2565 Old Milton Pkwy, Alpharetta, GA 30009	VersaLink C505	3RB731582	Color	150	\$0.0700	\$10.50
Public Works	Public Works Headquarters	1790 Hembree Rd, Alpharetta, GA 30009	WorkCentre 6505/DN	YTB116929	B\W	250	\$0.0135	\$3.38
Public Works	Public Works Headquarters	1790 Hembree Rd, Alpharetta, GA 30009	WorkCentre 6505/DN	YTB116929	Color	150	\$0.0700	\$10.50
Recreation, Parks & Cultural Services	Alpharetta Community Center	175 Roswell St, Alpharetta, GA 30009	WorkCentre 6505/N	YRB112799	B\W	200	\$0.0135	\$2.70
Recreation, Parks & Cultural Services	Alpharetta Community Center	175 Roswell St, Alpharetta, GA 30009	WorkCentre 6505/N	YRB112799	Color	216	\$0.0700	\$15.12
Public Safety	Public Safety Training Center	11565 Maxwell Rd, Alpharetta, GA 30009	WorkCentre 6515	5AV812964	B\W	200	\$0.0135	\$2.70
Public Safety	Public Safety Training Center	11565 Maxwell Rd, Alpharetta, GA 30009	WorkCentre 6515	5AV812964	Color	150	\$0.0700	\$10.50
Recreation, Parks & Cultural Services	Equestrian Center	11915 Wills Rd, Alpharetta, GA 30009	WorkCentre 6515	5AV811913	B\W	1,190	\$0.0135	\$16.07
Recreation, Parks & Cultural Services	Equestrian Center	11915 Wills Rd, Alpharetta, GA 30009	WorkCentre 6515	5AV811913	Color	150	\$0.0700	\$10.50
Public Safety	Fire Station 81	2970 Webb Bridge Rd, Alpharetta, GA 30009	WorkCentre 6605	XL3583543	B\W	548	\$0.0135	\$7.40
Public Safety	Fire Station 81	2970 Webb Bridge Rd, Alpharetta, GA 30009	WorkCentre 6605	XL3583543	Color	175	\$0.0700	\$12.25
Public Safety	Public Safety Headquarters	2565 Old Milton Pkwy, Alpharetta, GA 30009	WorkCentre 6605/DN	XL3569201	B\W	200	\$0.0135	\$2.70

RFP 22-124 (Managed Print Services)

EDGE Business Systems

Print Fleet and Monthly Usage Patterns

Department	Facility	Facility Address	Machine Type	Serial Number	Meter Type	Monthly Volume Snapshot	Cost Per Page	Monthly Usage Cost
Public Safety	Public Safety Headquarters	2565 Old Milton Pkwy, Alpharetta, GA 30009	WorkCentre 6605/DN	XL3569201	Color	150	\$0.0700	\$10.50
Public Safety	Public Safety Headquarters	2565 Old Milton Pkwy, Alpharetta, GA 30009	WorkCentre 6605/DN	XL3581156	B\W	310	\$0.0135	\$4.19
Public Safety	Public Safety Headquarters	2565 Old Milton Pkwy, Alpharetta, GA 30009	WorkCentre 6605/DN	XL3581156	Color	236	\$0.0700	\$16.52
City Administration	City Hall	2 Park Plaza, Alpharetta GA 30009	WorkCentre 6605/DNM	XL3566562	B\W	200	\$0.0135	\$2.70
City Administration	City Hall	2 Park Plaza, Alpharetta GA 30009	WorkCentre 6605/DNM	XL3566562	Color	150	\$0.0700	\$10.50
Information Technology	City Hall	2 Park Plaza, Alpharetta GA 30009	WorkCentre 6605/DNM	XL3566105	B\W	200	\$0.0135	\$2.70
Information Technology	City Hall	2 Park Plaza, Alpharetta GA 30009	WorkCentre 6605/DNM	XL3566105	Color	150	\$0.0700	\$10.50
Public Safety	Public Safety Headquarters	2565 Old Milton Pkwy, Alpharetta, GA 30009	WorkCentre 6605/DNM	XL3567252	B\W	371	\$0.0135	\$5.01
Public Safety	Public Safety Headquarters	2565 Old Milton Pkwy, Alpharetta, GA 30009	WorkCentre 6605/DNM	XL3567252	Color	223	\$0.0700	\$15.61
Public Safety	Fire Station 83	9600 Westside Pkwy, Alpharetta, GA 30009	WorkCentre 6605/DNM	XL3570865	B\W	281	\$0.0135	\$3.79
Public Safety	Fire Station 83	9600 Westside Pkwy, Alpharetta, GA 30009	WorkCentre 6605/DNM	XL3570865	Color	150	\$0.0700	\$10.50
Public Safety	Public Safety Headquarters	2565 Old Milton Pkwy, Alpharetta, GA 30009	WorkCentre 6605/DNM	XL3570866	B\W	200	\$0.0135	\$2.70
Public Safety	Public Safety Headquarters	2565 Old Milton Pkwy, Alpharetta, GA 30009	WorkCentre 6605/DNM	XL3570866	Color	150	\$0.0700	\$10.50
Public Safety	Fire Station 86	3275 Kimball Bridge Rd, Alpharetta, GA 30022	WorkCentre 6605/DNM	XL3581067	B\W	200	\$0.0135	\$2.70
Public Safety	Fire Station 86	3275 Kimball Bridge Rd, Alpharetta, GA 30022	WorkCentre 6605/DNM	XL3581067	Color	150	\$0.0700	\$10.50
Public Safety	Public Safety Headquarters	2565 Old Milton Pkwy, Alpharetta, GA 30009	WorkCentre 6605/DNM	XL3597525	B\W	316	\$0.0135	\$4.27
Public Safety	Public Safety Headquarters	2565 Old Milton Pkwy, Alpharetta, GA 30009	WorkCentre 6605/DNM	XL3597525	Color	150	\$0.0700	\$10.50
Public Safety	Public Safety Substation	92 Milton Ave, Suite 100, Alpharetta, GA 30009	WorkCentre 6605/DNM	XL3602946	B\W	200	\$0.0135	\$2.70
Public Safety	Public Safety Substation	92 Milton Ave, Suite 100, Alpharetta, GA 30009	WorkCentre 6605/DNM	XL3602946	Color	150	\$0.0700	\$10.50
Court	Municipal Court	13690 Highway 9 (Building B), Milton, GA 30004	WorkCentre 6655	X7P000651	B\W	200	\$0.0135	\$2.70
Court	Municipal Court	13690 Highway 9 (Building B), Milton, GA 30004	WorkCentre 6655	X7P000651	Color	150	\$0.0700	\$10.50
Public Works	Public Works Headquarters	1790 Hemtree Rd, Alpharetta, GA 30009	WorkCentre 7120	XDC115514	B\W	608	\$0.0135	\$8.21
Public Works	Public Works Headquarters	1790 Hemtree Rd, Alpharetta, GA 30009	WorkCentre 7120	XDC115514	Color	200	\$0.0700	\$14.00
Community & Economic Development	City Hall	2 Park Plaza, Alpharetta GA 30009	WorkCentre 7220	LX7380598	B\W	915	\$0.0135	\$12.35
Community & Economic Development	City Hall	2 Park Plaza, Alpharetta GA 30009	WorkCentre 7220	LX7380598	Color	150	\$0.0700	\$10.50
Public Works	Public Works Headquarters	1790 Hemtree Rd, Alpharetta, GA 30009	WorkCentre 7830	MX1220560	B\W	1,080	\$0.0135	\$14.57
Public Works	Public Works Headquarters	1790 Hemtree Rd, Alpharetta, GA 30009	WorkCentre 7830	MX1220560	Color	1,025	\$0.0700	\$71.75
Recreation, Parks & Cultural Services	City Hall	2 Park Plaza, Alpharetta GA 30009	WorkCentre 7835	MX1193348	B\W	1,088	\$0.0135	\$14.69
Recreation, Parks & Cultural Services	City Hall	2 Park Plaza, Alpharetta GA 30009	WorkCentre 7835	MX1193348	Color	951	\$0.0700	\$66.57
Community & Economic Development	City Hall	2 Park Plaza, Alpharetta GA 30009	WorkCentre 7845	MX4482648	B\W	1,744	\$0.0135	\$23.54
Community & Economic Development	City Hall	2 Park Plaza, Alpharetta GA 30009	WorkCentre 7845	MX4482648	Color	465	\$0.0700	\$32.55
Public Safety	Public Safety Headquarters	2565 Old Milton Pkwy, Alpharetta, GA 30009	WorkCentre 7845	MX4496499	B\W	1,598	\$0.0135	\$21.57
Public Safety	Public Safety Headquarters	2565 Old Milton Pkwy, Alpharetta, GA 30009	WorkCentre 7845	MX4496499	Color	633	\$0.0700	\$44.31
Public Safety	Public Safety Headquarters	2565 Old Milton Pkwy, Alpharetta, GA 30009	WorkCentre 7845	MX4328645	B\W	228	\$0.0135	\$3.08
Public Safety	Public Safety Headquarters	2565 Old Milton Pkwy, Alpharetta, GA 30009	WorkCentre 7845	MX4328645	Color	150	\$0.0700	\$10.50
Public Safety	Public Safety Headquarters	2565 Old Milton Pkwy, Alpharetta, GA 30009	WorkCentre 7855	MX4351838	B\W	1,374	\$0.0135	\$18.55
Public Safety	Public Safety Headquarters	2565 Old Milton Pkwy, Alpharetta, GA 30009	WorkCentre 7855	MX4351838	Color	1,493	\$0.0700	\$104.51
Recreation, Parks & Cultural Services	City Hall	2 Park Plaza, Alpharetta GA 30009	C405 - NEW Jan 2022	4HX595304	BW	515	\$0.0135	\$6.95
Finance	City Hall	2 Park Plaza, Alpharetta GA 30009	Phaser 3260	K8A231105	B\W	350	\$0.0135	\$4.73
Finance	City Hall	2 Park Plaza, Alpharetta GA 30009	Phaser 3260	K8A231222	B\W	350	\$0.0135	\$4.73
Finance	City Hall	2 Park Plaza, Alpharetta GA 30009	Phaser 3260	K8A231226	B\W	350	\$0.0135	\$4.73
Public Safety	Public Safety Headquarters	2565 Old Milton Pkwy, Alpharetta, GA 30009	Phaser 3260	K8A262800	B\W	350	\$0.0135	\$4.73
Public Safety	Public Safety Headquarters	2565 Old Milton Pkwy, Alpharetta, GA 30009	Phaser 3260	K8A262809	B\W	350	\$0.0135	\$4.73
Court	Municipal Court	13690 Highway 9 (Building B), Milton, GA 30004	Phaser 3320	LA2577215	B\W	350	\$0.0135	\$4.73
Court	Municipal Court	13690 Highway 9 (Building B), Milton, GA 30004	Phaser 3320	LA2577227	B\W	350	\$0.0135	\$4.73
Public Safety	Jail Facility	2555 Old Milton Pkwy, Alpharetta, GA 30009	Phaser 3320	LA2288869	B\W	350	\$0.0135	\$4.73
Public Safety	Public Safety Headquarters	2565 Old Milton Pkwy, Alpharetta, GA 30009	Phaser 3320	LA2579387	B\W	908	\$0.0135	\$12.26
Human Resources	City Hall	2 Park Plaza, Alpharetta GA 30009	Phaser 3330	9BR548404	B\W	350	\$0.0135	\$4.73
Public Safety	Public Safety Headquarters	2565 Old Milton Pkwy, Alpharetta, GA 30009	Phaser 3330	9BR371782	B\W	350	\$0.0135	\$4.73
Public Safety	Public Safety Headquarters	2565 Old Milton Pkwy, Alpharetta, GA 30009	Phaser 3330	9BR378240	B\W	350	\$0.0135	\$4.73
Public Safety	Public Safety Headquarters	2565 Old Milton Pkwy, Alpharetta, GA 30009	Phaser 3330	9BR378247	B\W	350	\$0.0135	\$4.73
Public Safety	Public Safety Headquarters	2565 Old Milton Pkwy, Alpharetta, GA 30009	Phaser 3330	9BR535551	B\W	350	\$0.0135	\$4.73
Public Safety	Public Safety Headquarters	2565 Old Milton Pkwy, Alpharetta, GA 30009	Phaser 3330	9BR538221	B\W	350	\$0.0135	\$4.73
Public Safety	Public Safety Headquarters	2565 Old Milton Pkwy, Alpharetta, GA 30009	Phaser 3330	9BR538864	B\W	350	\$0.0135	\$4.73
Public Safety	Public Safety Headquarters	2565 Old Milton Pkwy, Alpharetta, GA 30009	Phaser 3330	9BR538872	B\W	350	\$0.0135	\$4.73
Public Safety	Public Safety Headquarters	2565 Old Milton Pkwy, Alpharetta, GA 30009	Phaser 3330	9BR540701	B\W	350	\$0.0135	\$4.73

RFP 22-124 (Managed Print Services)

EDGE Business Systems

Print Fleet and Monthly Usage Patterns

Department	Facility	Facility Address	Machine Type	Serial Number	Meter Type	Monthly Volume Snapshot	Cost Per Page	Monthly Usage Cost
Recreation, Parks & Cultural Services	Alpharetta Community Center	175 Roswell St, Alpharetta, GA 30009	Phaser 3330	9BR371782	B\W	350	\$0.0135	\$4.73
City Administration	City Hall	2 Park Plaza, Alpharetta GA 30009	Phaser 6510	4AV770208	n/a	350	\$0.0135	\$4.73
Finance	City Hall	2 Park Plaza, Alpharetta GA 30009	VersaLink B400	6HB838975	B\W	350	\$0.0135	\$4.73
Public Works	Public Works Headquarters	1790 Hembree Rd, Alpharetta, GA 30009	VersaLink B400	6HB027467	B\W	350	\$0.0135	\$4.73
City Administration	City Hall	2 Park Plaza, Alpharetta GA 30009	WorkCentre 3325	LA8669819	B\W	350	\$0.0135	\$4.73
Public Safety	Fire Station 84	525 Park Bridge Pkwy, Alpharetta, GA 30005	WorkCentre 3325	LA8192423	B\W	350	\$0.0135	\$4.73
Public Safety	Fire Station 85	1475 Mid Broadwell Rd, Alpharetta, GA 30004	WorkCentre 3325	LA8666597	B\W	350	\$0.0135	\$4.73
Public Safety	Fire Station 86	3275 Kimball Bridge Rd, Alpharetta, GA 30022	WorkCentre 3325	LA8666620	B\W	350	\$0.0135	\$4.73
Public Safety	Jail Facility	2555 Old Milton Pkwy, Alpharetta, GA 30009	WorkCentre 3325	LA8671356	B\W	350	\$0.0135	\$4.73
Recreation, Parks & Cultural Services	Rock Mill Park	3100 Kimball Bridge Rd, Alpharetta, GA 30022	WorkCentre 3335	5BT727747	n/a	350	\$0.0135	\$4.73
Public Safety	Fire Station 83	9600 Westside Pkwy, Alpharetta, GA 30009	WorkCentre 3550/X	VMA574031	B\W	683	\$0.0135	\$9.22
Public Safety	Fire Station 82	3070 Market Pl, Alpharetta, GA 30005	WorkCentre 3550/X	VMA672447	B\W	335	\$0.0135	\$4.52
Recreation, Parks & Cultural Services	Equestrian Center	11915 Wills Rd, Alpharetta, GA 30009	WorkCentre 6515	5AV812616	n/a	350	\$0.0135	\$4.73
Public Safety	Public Safety Headquarters	2565 Old Milton Pkwy, Alpharetta, GA 30009	WorkCentre 6605/DNM	XL3579711	n/a	350	\$0.0135	\$4.73
Court	Municipal Court	13690 Highway 9 (Building B), Milton, GA 30004	Phaser 3610/DN	A4T020246	B\W	465	\$0.0135	\$6.28

Total Monthly Cost based on volume snapshot \$2,248.53

Total Annual Cost based on volume snapshot \$26,982.35

MFPs and Printers

BW Quarterly copy/prints included

BW Overages

120,000

\$0.0135

BW Annual copy/prints included

480,000

\$0.0135

Note: Under EDGE Management, City of Alpharetta will be able to change volumes quarterly based on actual usage trends. Furthermore, EDGE offers to set up all copying and printing to default to black/white which will reduce overall monthly cost

Color Quarterly copy/prints included

Color Overages

60,000

\$0.07

Color Annual copy/prints included

240,000

\$0.07

Note: Quarterly and Annual proposed is all-inclusive of all service, consumable supplies (except paper & staples)



CITY OF ALPHARETTA REQUEST FOR PROPOSALS (RFP)

RFP Number: 22-124

RFP Title: Managed Print Services

RFP SCOPE OF WORK & PROPOSAL SUBMISSION

1. RFP Period of No Communication

The no communication period starts on the issue date of this RFP June 23, 2022 and lasts until the City Council meeting for contract award recommendation (or until contract award if this isn't required to go before council for approval).

Any person or company, their employees, representatives, agents, attorneys, etc. must not contact the City's elected officials or any City staff concerning this RFP.

Contacting anyone other than the Procurement Agent named below for this RFP during this time will be reason to remove a proposal from review.

2. Procurement Agent, Single Point of Contact

Debora Westbrook is the Procurement Agent and Single Point of Contact for this RFP and is the only contact representing the City for this RFP.

Enter all questions or comments using Opportunity Q&A tab at the Bonfire project web page. Debora can be reached at 678-297-6052 or purchasing@alpharetta.ga.us.

City of Alpharetta
2 Park Plaza
Alpharetta, GA 30009
Attn: Debora Westbrook, Procurement Agent

3. RFP Schedule of Events

1. **Proposal Close Date, Deadline for Submissions: July 21, 2022 at 10:00 AM.** We may change this date during the RFP process. We will post any change in an addendum. Review web page for addenda.
2. Link to Bonfire Project Web Page: <https://cityofalpharetta.bonfirehub.com/>
3. This project web page has the important dates and all project documents for this RFP.
4. Enter all questions, comments, requests for information before the Questions Due Date using ☒ **Message – Opportunity Q&A** at the project web page.
5. In each question, clearly tell the RFP document and section that is in question.
6. We will share any changes or added information from the City by a written addendum. We will make the information available to the public on the project web page.
7. It is your responsibility to check the project web page for any addenda, other information, or other messages before finally uploading a proposal. You must respond using any updated information.

4. Our Review of Proposals and Review Criteria:

1. The City will make investigations as we feel necessary to make sure of the Offeror's ability to provide the supplies or perform the work or services detailed in this RFP.
2. We will first review all proposals to be sure that proposal have basic requirements and information.
3. Some scoring may simply be Pass/Fail. Any proposal that Fails any part or section that is needed will be removed from further review and scoring.
4. The Review Team will only get correct proposals for review and scoring. Proposals will be scored based on the evaluation criteria below. We may consider accepted industry standards. We may compare all proposals to each other for price, quality, quantity, contract terms, etc. We will use this review and scoring to decide the top-scoring proposal[s] and the best value for our City.
5. The Review Team may decide to create a shortlist of the top-scoring proposals. If so, the shortlisted firms may be invited for a presentation or interview with us; may be asked to set-up a site visit; or may be asked to supply more information for review. We may ask for discussion, negotiation, or a "best and final offer" to finally decide the highest-scoring proposal.
6. We will review and score each proposal using the criteria and percentage weights below:
 - a. Cover letter, business profile, and business information is required but not scored.
 - b. Required Forms are Pass/Fail.
 - c. Questionnaire scoring will depend on information requested. Some questionnaire responses will be information only, while others may be pass fail such as addendum acknowledgement.

Evaluation Criteria	Maximum Points
Technical Proposal	70
(1) compatibility with the City's desired functional and technical requirements and (2) compatibility with current and future technological infrastructure.	25
Proposed staffing approach, qualifications of proposed staff maintenance, and support program, etc.	25
Company background, client references, experience, and customer service rating.	20
Local Vendor Preference	3
Annual cost proposal given the City's equipment and print volume. (Please refer to the Excel file titled Print Fleet and Monthly Usage Patterns.)	27
Total Maximum point score	100

7. If the City desires, the highest scoring firms will be shortlisted and invited to participate in a second phase consisting of an interview and presentation. The scoring for this Phase 2 will be 100 maximum points for the presentation and interview. For shortlisted firms, Phase 2 evaluation will be stand-alone final scoring.

8. If the City elects to move forward with the Phase 2 evaluation, shortlisted firms will be notified by close of business on Friday, August 5, 2022. We will plan to conduct interviews between August 15 and August 26, 2022.
9. In the event the City elects not to move forward with Phase 2, Phase 1 scoring will stand as the sole scoring criteria.
10. If the City is unable to complete negotiations with the highest scoring firm, the City will then move to the next high scoring firm for negotiations. An actual contract award is subject to successful cost negotiation with the successful consultant.

WHAT WE WANT TO DO

1. General Description

The City of Alpharetta is requesting proposals from qualified vendors to provide Managed Print Services for our existing fleet of approximately 105 printers and multi-function devices. Devices are a range of types and may be either Black/White print only or may print Black/White and Color. The City has standardized with Xerox equipment.

Services will include on-site service, parts and consumable supplies.

2. About our City

Drawing from its beginnings in 1858 when incorporated as the Milton County seat, The City of Alpharetta boasts a history of enterprise, growth, and prosperity, thus enriching the lives of residents and the many people visiting and working in our city.

Alpharetta is one of fifteen incorporated cities/towns within Fulton County and is one of the fastest growing communities in the South. It is situated in North Fulton County about 25 miles north of the City of Atlanta and about 35 miles from the Hartsfield-Jackson Atlanta International Airport, the world's busiest airport. Our City occupies a land area of about 27 square miles and serves an estimated population of 65,799 (population) and 84,817 (workforce). The City government employs a full-time equivalent of approximately 445 positions (not including seasonal positions).

Alpharetta is a beautiful and vibrant Southern city offering a unique blend of excellent schools, incredible job opportunities, diverse shopping choices, convenience to first-rate healthcare, cultural and recreational events, and abundant green space. It's no wonder Alpharetta is one of the hottest markets in both commercial, retail, and residential real estate. Through all its progress, the city has kept its down-to-earth character. Which may be why people who live here usually stay here. And why there's always something new and exciting happening.

During the late-1990s, the City of Alpharetta started to grow its infrastructure from the ground up—literally. Hundreds of miles of fiber optic cables were buried throughout the city. The State's largest electricity provider, Georgia Power, took it a step further by setting up a series of redundant electric networks throughout the city. The result being that Alpharetta's technological infrastructure is the ideal environment for tech companies and the tech needs of any company. You won't find more fertile ground for your business to grow.

Folks in our city understand the value and benefits of recreation and parks, both in their personal lives and to our community as a whole. Alpharetta has an exceptional park system that truly enhances the

quality of life in our City. Located all around the City, there are over 830 acres devoted to walking trails, playgrounds, sports fields, arboretums, and community parks. At the expansive Wills Park, along with excellent sports and recreational facilities, you'll find one of the finest equestrian facilities in the Southeast. Alpharetta also has a beautiful greenway system along Big Creek that provides a naturally picturesque pathway for bikers and hikers of all ages to enjoy

3. Scope of Work

A. Minimum Requirements:

- a. Must be authorized by the Xerox to service and support the entire product line.
- b. Must be factory trained and certified.
- c. Technicians must be vetted through GCIC.
 - Vendor and its employees must agree to a Non-Criminal Justice CJIS Network & Data Agreement.
 - Vendor must maintain and manage their employees' GCIC required training and provide training records upon request.
- d. Only genuine OEM parts and consumables will be used.
- e. Must have at least one physical location with OEM parts and consumables within 30 miles of Alpharetta City Hall, 2 Park Plaza, Alpharetta, GA.
- f. Required to install, train, and support any 3rd party software proposed.
- g. Average time between placing a service call or support email and service technician or dispatch agent response contact to Information Technology Department or point of contact at the device location will be within 2 hours
- h. The City expects equipment to be repaired within one (1) day.
 - If a device cannot be repaired a loaner device must be provided meeting the previous devices specifications as to not interrupt workflow.
- i. Supplies distribution chain to designated print administrators for each department.

B. Technology

The City's Information Technology (IT) department uses PrinterLogic for remote driver installation. The proposed management system must not interfere with PrinterLogic . It must enhance or replace the current feature offerings.

The City does not currently use the secure print release functionality available with PrinterLogic.

Any proposed print management software must include secure print release functionality as well as copy/scan tracking for accurate report audits.

- a. Propose a new Print Management / Deployment Software – (please include white papers and any detailed collateral information in response)
- b. Minimum Print Management Software Requirements:

- A minimum of 1 software upgrade per year to keep up with vulnerability patches and bug fixes.
 - Software versions across all devices in the field within the respective device families need to be uniform.
 - Provide centralized security and configuration management for all devices.
 - Must be able to provide Paper Cut integration and in-house support.
 - Must be able to provide Azure integration and in-house support.
- c. Enable Find-Me / Secure Print release – Documents printed for any of the devices must be able to print to a virtual queue and have their jobs released at any device in the fleet.
- d. Technical Requirement to meet upcoming IT needs:
- SSO Integration for Office365 Apps.
 - Secure badge release printing using badge ID integration within AD via our future Badge management system Avigilon.
 - Must propose options to enhance or replace existing EFAX solution and to integrate secure fax lines.

C. Proposal Response Requirements

Invoice Requirements – The City requires one itemized monthly invoice with all devices listed and with a minimum of the following information for each device:

- Equipment model and number
 - Department
 - Location within Department
 - IP address
 - starting meters BW/Color
 - end meter BW/Color
 - Cost x impression
 - Cost per usage per machine.
- D. If proposing volume-based pricing, the City desires to have overages/underages (if any) to be reconciled quarterly.
- E. Active Account Management with Reporting and Quarterly Reviews – The City of Alpharetta requires the vendors to provide quarterly performance and service reviews and recommendations in-person (unless specified by the City of Alpharetta) no later than 2-weeks after the end of the quarter. Please include actual sample review reports.
- F. Detailed Information on service process – Please elaborate in detail. Include specifics on the process, capabilities, on-site response time, and service reviews sample reports.
- G. Detailed Information on the consumable supplies (everything except paper & staples) order and fulfillment process.

- H. Detailed Information on proposed Print Management Software proposed – Include detailed specifications and white papers, brochures, implementation, support, and training procedures.
- I. Exceptions – Include commentary on any exceptions to the specifications that you are making in the response. For example, if a particular model is discontinued and/or OEM parts and supplies are not readily available to meet the respondent Service Level Agreement.
- J. Optional Values Added hardware/software solutions not requested - In this section please include options for features not requested or considered that your company feels are relevant. You may include a detailed spreadsheet of charges in a separate tab to the Pricing Sheet.
- K. Print Management Software Specifications– Include any relevant brochures and/or explanations of functionality requested according to technology and finance requirements. Include this information in an appendix to the Technical Proposal response. References to materials included should be included within the Technical Proposal.

FOLLOW THIS OUTLINE

How We Want You to Construct Your Proposal

1. Using Bonfire to Submit Proposal

- 1.1. This is the link to Bonfire Project Web Page to get our documents and to upload your proposal: <https://cityofalpharetta.bonfirehub.com/>
- 1.2. We are accepting all proposals by online response only. You must upload completed proposals online before the closing date and time found in Project Details of the project web page for this RFP.
- 1.3. Don't send proposals by mail, fax, or email. We will not accept paper copy proposals. We will not accept any proposals after the closing time deadline has passed.
- 1.4. You have not completed your response simply by uploading proposal documents and information. You must successfully upload all the required documents, including filling out any questionnaires, price sheets, or data requests, and then you must click the submit button before the closing time.
- 1.5. You will receive an email confirmation receipt with a unique confirmation number shortly after you complete your proposal upload. This confirms that you have successfully turned in your proposal with all required information.
- 1.6. You can update your proposal at any time until the closing time.
- 1.7. All uploaded items and responses are Sealed and will only be visible by the City after the closing time has passed.
- 1.8. If the file is 'mandatory' or 'required', you won't be able to complete your proposal until you have met all requirements.

- 1.9. Uploading large documents may take more time, depending on the size of the file(s) and your Internet connection speed.
- 1.10. Pay attention to the type and number of files we have asked you to upload.
- 1.11. The largest upload file size is 1000 MB.
- 1.12. Don't embed any documents within your uploaded files. They won't be accessible or evaluated.
- 1.13. Minimum system requirements: Internet Explorer 11, Microsoft Edge, Google Chrome, or Mozilla Firefox. Java Script must be enabled.

2. Required Proposal Document Formats

- ❖ Each proposal must follow these document formats.
 - Failure to follow these formats will reduce our review team's ability to evaluate and will result in a lower proposal score or in complete removal of a proposal from scoring.
 - Format your documents using this outline:
 - ☐ formatted to single space lines,
 - ☐ 10 to 12-point font size,
 - ☐ black font color, and
 - ☐ upload proposal in PDF format.

COMPANY INFORMATION

Required but no points assigned.

- This document must be no more than two (2) pages,
- Each section below will make up the Company Information document. This document must be in the following order:
 - A. **Cover Letter with Brief Business Profile**, length of time in business, and a summary describing company strong points and why your experience with similar projects will benefit the City.
 - B. **Business information**, including name and home office address. If another office address oversees work of this project, add that address information too.
 - C. **Contact**, one person to be the single point of contact for this proposal. All communication with the City will be with this person. Supply the following contact information in the proposal:
 - Name, including business title and preferred name prefix (EX: Mr. Ms. Dr. etc.)
 - mailing address,
 - telephone number, cell phone number, and
 - e-mail address.

TECHNICAL PROPOSAL **70 Points**

- This document must be no more than fifteen (15) pages,

- A. **Requirements: Discuss with enough detail to explain:**
- i. Compatibility with the City's desired functional and technical requirements, and
 - ii. Compatibility with current and future technological infrastructure.
- B. **Proposed staffing approach:**
- a. Provide an organizational chart for the project team.
 - b. Identify the following team members/contacts with the City:
 1. Team leader
 2. Key Personnel/Technicians
 - c. For each individual listed above, answer the following questions. Please use a separate page for each team member.
 1. Where is this individual located?
 2. How long has this individual been employed by this respondent?
 3. Years of experience?
 4. Licenses or accreditation?
 5. What is the availability of this individual to devote time to the project?
 6. What is this individual's length of experience with the project team?
 7. Give 3 examples of specific experience relevant to this project.
 - d. Provide one-page resumes for all key personnel.
 - e. Discuss how the location of the respondent and project staff will impact the service to our City and the coordination with the City's staff.
- iii. Maintenance and support program, provide details.
- C. **Company background, experience, client references, customer service rating.**
- a. Profile company history and background. At the least, include:
 1. Number of years in business,
 2. Current locations
 3. Number of personnel employed
 4. Experience with Managed Print Service such as we are requesting in the RFP, especially working with similar sized entities.
 5. Note any customer service ratings for satisfaction reports that are from independent and verifiable sources.
 - b. Supply at least three references for work or services like the project in this RFP (don't include the City of Alpharetta). These references must be for work or services provided within the last three years. At a minimum, provide for each reference:

1. Company name,
2. Company address,
3. Contact name,
4. Contact email address, and
5. Contact phone number in your response.

NOTE: We contact references to verify your ability to do the work. We also reserve the right to use any information or other references to decide your ability to perform the work in this RFP. Poor references from any source are grounds to disqualify a proposal.

COST PROPOSAL 27 Points

A. Annual Cost including print volume and base charge.

Based on equipment list and monthly usage chart provided, provide a detailed cost proposal to the City. Printer inventory and Volumes is provided in Appendix A and included as a separate spreadsheet, Print Fleet and Monthly Usage Patterns, that lists our current printer fleet and as an example of our past usage.

Cost proposal will be evaluated on the Total Annual Cost as estimated in vendor's cost proposal using the monthly usage we have provided. We realize that actual annual costs may differ.

REQUIRED FORMS

- We have provided a document file with three required forms. You must complete these forms and return to us with every proposal.
- We prefer all three completed forms returned as one PDF file. However, we won't lower your scoring if you return the forms separately.
- Below are the required forms for all proposals:
 - A. **IRS Form W-9**
 - B. **Bidder's Disclosures and Certifications**
 - C. **E-Verify** (Affidavit Verifying Contractor Participation in Federal Work Authorization Program)

- ❖ *E-Verify side note:* Companies return this form to us incorrectly more often than anything else we request in our RFPs.
 - ❖ Top mistakes include wrong number or missing information.
 - ❖ State of Georgia law requires that we have this completed form before we can review a bid or proposal.
 - ❖ A form with errors doesn't fulfill this requirement.

All the following must be on the E-verify affidavit.

- Federal Work Authorization User Identification Number – this is only five to eight numbers.
 - ⊗ No A,B,Cs.
 - ⊗ It's different from your Tax ID, Employer Identification, or Social Security Number.
 - ⊗ It won't have a combination of letters and numbers.
- Date of Authorization – this is when you first signed up and got the E-verify number.
- Name of Contractor – your company
- Name of Project – Same as RFP title
- Date, City, and State – when and where this form was signed
- Signature of Authorized Officer or Agent – to be signed
- Printed Name and Title of Authorized Officer or Agent – the person that signed the form.
- Notarized with seal

D. Local Vendor Preference application is not a required document. 3 Points

Only if your company fits the requirements for a City of Alpharetta Local Vendor, provide the completed application along with all requested information/ documents.

QUESTIONNAIRE

We use a questionnaire to gather important information needed for legal requirements, your acknowledgements, our proposal review, or information needed for writing a contract.

Some questions may require your answers about the work we have described in this RFP.

You will fill out the questionnaire provided. There is no other form or document to upload.

Information requests and response types are as follows:

- Authorized signer for contract execution in DocuSign: Name, business title, email address, Response Type: Response Type: text entry.
- Corporate secretary for contract execution in DocuSign: Name, business title, email address, Response Type: Response Type: text entry.
- Legal notices contact needed for contracting: Business name and mailing address, contact name, Response Type: text entry.
- Unique Entity ID / identifier used at SAM.gov, Response Type: alphanumeric entry.
- Addenda Acknowledgement, enter the number of addenda received: Response Type: 0, 1, 2, etc.
- Insurance Requirement Acknowledgement, Response Type: Yes, No entry.

APPENDIX A: PRINT INVENTORY AND VOLUMES

Monthly Volume Snapshot may not represent actual usage for any machine listed.
Certain machine listed may in use, but not in the network.

Department	Facility	Machine Type	Serial Number	Meter Type	Monthly Volume Snapshot
Recreation, Parks & Cultural Services	Arts Center	AltaLink C8035	3TX396961	B\W	576
Recreation, Parks & Cultural Services	Arts Center	AltaLink C8035	3TX396961	Color	832
City Administration	City Hall	AltaLink C8045	8TB604952	B\W	873
City Administration	City Hall	AltaLink C8045	8TB604952	Color	3,152
Recreation, Parks & Cultural Services	Wills Park Recreation Center	AltaLink C8045	8TB603958	B\W	965
Recreation, Parks & Cultural Services	Wills Park Recreation Center	AltaLink C8045	8TB603958	Color	294
Recreation, Parks & Cultural Services	Adult Activity Center	AltaLink C8055	8TB600778	B\W	1,178
Recreation, Parks & Cultural Services	Adult Activity Center	AltaLink C8055	8TB600778	Color	666
Community & Economic Development	City Hall	AltaLink C8070	6TB447421	B\W	3,274
Community & Economic Development	City Hall	AltaLink C8070	6TB447421	Color	2,768
Finance	City Hall	AltaLink C8070	6TB447291	B\W	4,140
Finance	City Hall	AltaLink C8070	6TB447291	Color	2,275
Court	Municipal Court	AltaLink C8135	ELQ514699	B\W	2,806
Court	Municipal Court	AltaLink C8135	ELQ514699	Color	1,234
Public Safety	Public Safety Headquarters	ColorQube 8570/DN	XFN138485	B\W	200
Public Safety	Public Safety Headquarters	ColorQube 8570/DN	XFN138485	Color	150
Recreation, Parks & Cultural Services	Equestrian Center	ColorQube 8570/DNM	XFN138476	B\W	200
Recreation, Parks & Cultural Services	Equestrian Center	ColorQube 8570/DNM	XFN138476	Color	150
Information Technology	City Hall	ColorQube 8570/DT	XFN101720	BW Useful Color	200
Information Technology	City Hall	ColorQube 8570/DT	XFN101720	Color2	150
Recreation, Parks & Cultural Services	Crabapple Government Center	ColorQube 8700/XF	DA3000650	BW Useful Color	200
Recreation, Parks & Cultural Services	Crabapple Government Center	ColorQube 8700/XF	DA3000650	Color2	150
Recreation, Parks & Cultural Services	Crabapple Government Center	ColorQube 8700/XF	DA3000650	Color3	150
Public Safety	Public Safety Headquarters	ColorQube 8900/X	DA4107371	BW Useful Color	1,141
Public Safety	Public Safety Headquarters	ColorQube 8900/X	DA4107371	Color2	150
Public Safety	Public Safety Headquarters	Phaser 6022	P5A069246	B\W	200
Public Safety	Public Safety Headquarters	Phaser 6022	P5A069246	Color	150
Court	Municipal Court	VersaLink C400	7HB471184	B\W	200
Court	Municipal Court	VersaLink C400	7HB471184	Color	504
Finance	City Hall	VersaLink C400	7HB946305	B\W	583



Finance	City Hall	VersaLink C400	7HB946305	Color	249
Public Safety	Public Safety Headquarters	VersaLink C400	7HB780689	B\W	200
Public Safety	Public Safety Headquarters	VersaLink C400	7HB780689	Color	150
Finance	City Hall	VersaLink C405	4HX593106	B\W	200
Finance	City Hall	VersaLink C405	4HX593106	Color	150
Finance	City Hall	VersaLink C405	4HX593136	B\W	200
Finance	City Hall	VersaLink C405	4HX593136	Color	150
Finance	City Hall	VersaLink C405	4HX593142	B\W	200
Finance	City Hall	VersaLink C405	4HX593142	Color	150
Finance	City Hall	VersaLink C405	4HX813858	B\W	1,436
Human Resources	City Hall	VersaLink C405	4HX813858	Color	718
Public Safety	Public Safety Headquarters	VersaLink C405	4HX593107	B\W	2,438
Public Safety	Public Safety Headquarters	VersaLink C405	4HX593107	Color	124
Public Safety	Public Safety Headquarters	VersaLink C405	4HX593513	B\W	200
Public Safety	Public Safety Headquarters	VersaLink C405	4HX593513	Color	150
Public Safety	Public Safety Headquarters	VersaLink C405	4HX805542	B\W	254
Public Safety	Public Safety Headquarters	VersaLink C405	4HX805542	Color	150
Public Works	Public Works Headquarters	VersaLink C405	4HX593297	B\W	200
Public Works	Public Works Headquarters	VersaLink C405	4HX593297	Color	150
Recreation, Parks & Cultural Services	Wills Park Pool	VersaLink C405	4HX800561	B\W	554
Recreation, Parks & Cultural Services	Wills Park Pool	VersaLink C405	4HX800561	Color	150
Recreation, Parks & Cultural Services	City Hall	VersaLink C405	4HX816573	B\W	1,113
Recreation, Parks & Cultural Services	City Hall	VersaLink C405	4HX816573	Color	326
Public Safety	Public Safety Headquarters	VersaLink C505	3RB728688	B\W	154
Public Safety	Public Safety Headquarters	VersaLink C505	3RB728688	Color	319
Public Safety	Public Safety Headquarters	VersaLink C505	3RB731582	B\W	250
Public Safety	Public Safety Headquarters	VersaLink C505	3RB731582	Color	150
Public Works	Public Works Headquarters	WorkCentre 6505/DN	YTB116929	B\W	250
Public Works	Public Works Headquarters	WorkCentre 6505/DN	YTB116929	Color	150
Recreation, Parks & Cultural Services	Alpharetta Community Center	WorkCentre 6505/N	YRB112799	B\W	200
Recreation, Parks & Cultural Services	Alpharetta Community Center	WorkCentre 6505/N	YRB112799	Color	216
Public Safety	Public Safety Training Center	WorkCentre 6515	5AV812964	B\W	200
Public Safety	Public Safety Training Center	WorkCentre 6515	5AV812964	Color	150
Recreation, Parks & Cultural Services	Equestrian Center	WorkCentre 6515	5AV811913	B\W	1,190
Recreation, Parks & Cultural Services	Equestrian Center	WorkCentre 6515	5AV811913	Color	150
Public Safety	Fire Station 81	WorkCentre 6605	XL3583543	B\W	548
Public Safety	Fire Station 81	WorkCentre 6605	XL3583543	Color	175
Public Safety	Public Safety Headquarters	WorkCentre 6605/DN	XL3569201	B\W	200
Public Safety	Public Safety Headquarters	WorkCentre 6605/DN	XL3569201	Color	150
Public Safety	Public Safety Headquarters	WorkCentre 6605/DN	XL3581156	B\W	310



Public Safety	Public Safety Headquarters	WorkCentre 6605/DN	XL3581156	Color	236
City Administration	City Hall	WorkCentre 6605/DNM	XL3566562	B\W	200
City Administration	City Hall	WorkCentre 6605/DNM	XL3566562	Color	150
Information Technology	City Hall	WorkCentre 6605/DNM	XL3566105	B\W	200
Information Technology	City Hall	WorkCentre 6605/DNM	XL3566105	Color	150
Public Safety	Public Safety Headquarters	WorkCentre 6605/DNM	XL3567252	B\W	371
Public Safety	Public Safety Headquarters	WorkCentre 6605/DNM	XL3567252	Color	223
Public Safety	Fire Station 83	WorkCentre 6605/DNM	XL3570865	B\W	281
Public Safety	Fire Station 83	WorkCentre 6605/DNM	XL3570865	Color	150
Public Safety	Public Safety Headquarters	WorkCentre 6605/DNM	XL3570866	B\W	200
Public Safety	Public Safety Headquarters	WorkCentre 6605/DNM	XL3570866	Color	150
Public Safety	Fire Station 86	WorkCentre 6605/DNM	XL3581067	B\W	200
Public Safety	Fire Station 86	WorkCentre 6605/DNM	XL3581067	Color	150
Public Safety	Public Safety Headquarters	WorkCentre 6605/DNM	XL3597525	B\W	316
Public Safety	Public Safety Headquarters	WorkCentre 6605/DNM	XL3597525	Color	150
Public Safety	Public Safety Substation	WorkCentre 6605/DNM	XL3602946	B\W	200
Public Safety	Public Safety Substation	WorkCentre 6605/DNM	XL3602946	Color	150
Court	Municipal Court	WorkCentre 6655	X7P000651	B\W	200
Court	Municipal Court	WorkCentre 6655	X7P000651	Color	150
Public Works	Public Works Headquarters	WorkCentre 7120	XDC115514	B\W	608
Public Works	Public Works Headquarters	WorkCentre 7120	XDC115514	Color	200
Community & Economic Development	City Hall	WorkCentre 7220	LX7380598	B\W	915
Community & Economic Development	City Hall	WorkCentre 7220	LX7380598	Color	150
Community & Economic Development	City Hall	WorkCentre 7220	LX7380794	B\W	1,727
Community & Economic Development	City Hall	WorkCentre 7220	LX7380794	Color	157
Public Works	Public Works Headquarters	WorkCentre 7830	MX1220560	B\W	1,080
Public Works	Public Works Headquarters	WorkCentre 7830	MX1220560	Color	1,025
Recreation, Parks & Cultural Services	City Hall	WorkCentre 7835	MX1193348	B\W	1,088
Recreation, Parks & Cultural Services	City Hall	WorkCentre 7835	MX1193348	Color	951
Community & Economic Development	City Hall	WorkCentre 7845	MX4482648	B\W	1,744
Community & Economic Development	City Hall	WorkCentre 7845	MX4482648	Color	465
Public Safety	Public Safety Headquarters	WorkCentre 7845	MX4361472	B\W	1,534
Public Safety	Public Safety Headquarters	WorkCentre 7845	MX4361472	Color	150



Public Safety	Public Safety Headquarters	WorkCentre 7845	MX4496499	B\W	1,598
Public Safety	Public Safety Headquarters	WorkCentre 7845	MX4496499	Color	633
Public Safety	Public Safety Headquarters	WorkCentre 7845	MX4328645	B\W	228
Public Safety	Public Safety Headquarters	WorkCentre 7845	MX4328645	Color	150
Public Safety	Public Safety Headquarters	WorkCentre 7855	MX4351838	B\W	1,374
Public Safety	Public Safety Headquarters	WorkCentre 7855	MX4351838	Color	1,493
Recreation, Parks & Cultural Services	City Hall	C405 - NEW Jan 2022	4HX595304	BW	515
Finance	City Hall	Phaser 3260	K8A231105	B\W	350
Finance	City Hall	Phaser 3260	K8A231222	B\W	350
Finance	City Hall	Phaser 3260	K8A231226	B\W	350
Public Safety	Public Safety Headquarters	Phaser 3260	K8A262800	B\W	350
Public Safety	Public Safety Headquarters	Phaser 3260	K8A262809	B\W	350
Court	Municipal Court	Phaser 3320	LA2577161	B\W	586
Court	Municipal Court	Phaser 3320	LA2577215	B\W	350
Court	Municipal Court	Phaser 3320	LA2577220	B\W	350
Court	Municipal Court	Phaser 3320	LA2577223	B\W	350
Court	Municipal Court	Phaser 3320	LA2577227	B\W	350
Court	Municipal Court	Phaser 3320	LA2577499	B\W	350
Public Safety	Public Safety Headquarters	Phaser 3320	LA2200486	B\W	350
Public Safety	Jail Facility	Phaser 3320	LA2288869	B\W	350
Public Safety	Public Safety Headquarters	Phaser 3320	LA2579387	B\W	908
Human Resources	City Hall	Phaser 3330	9BR548404	B\W	350
Public Safety	Public Safety Headquarters	Phaser 3330	9BR371782	B\W	350
Public Safety	Public Safety Headquarters	Phaser 3330	9BR378240	B\W	350
Public Safety	Public Safety Headquarters	Phaser 3330	9BR378247	B\W	350
Public Safety	Public Safety Headquarters	Phaser 3330	9BR535551	B\W	350
Public Safety	Public Safety Headquarters	Phaser 3330	9BR535551	B\W	350
Public Safety	Public Safety Headquarters	Phaser 3330	9BR538221	B\W	350
Public Safety	Public Safety Headquarters	Phaser 3330	9BR538864	B\W	350
Public Safety	Public Safety Headquarters	Phaser 3330	9BR538866	B\W	350
Public Safety	Public Safety Headquarters	Phaser 3330	9BR538872	B\W	350
Public Safety	Public Safety Headquarters	Phaser 3330	9BR540701	B\W	350
Recreation, Parks & Cultural Services	Alpharetta Community Center	Phaser 3330	9BR371782	B\W	350
Recreation, Parks & Cultural Services	Arts Center	Phaser 3330	9BR381641	B\W	350
City Administration	City Hall	Phaser 6510	4AV770208	n/a	350
Finance	City Hall	VersaLink B400	6HB838975	B\W	350
Public Works	Public Works Headquarters	VersaLink B400	6HB027467	B\W	350
Public Safety	Fire Station 86	VersaLink B401	6HB042770	B\W	350
Recreation, Parks & Cultural Services	North Park	WorkCentre 3315	LA4228897	n/a	350
City Administration	City Hall	WorkCentre 3325	LA8669819	B\W	350



Public Safety	Fire Station 84	WorkCentre 3325	LA8192423	B\W	350
Public Safety	Fire Station 85	WorkCentre 3325	LA8666597	B\W	350
Public Safety	Fire Station 86	WorkCentre 3325	LA8666620	B\W	350
Public Safety	Jail Facility	WorkCentre 3325	LA8671356	B\W	350
Recreation, Parks & Cultural Services	Rock Mill Park	WorkCentre 3335	5BT727747	n/a	350
Public Safety	Fire Station 83	WorkCentre 3550/X	VMA574031	B\W	683
Public Safety	Fire Station 82	WorkCentre 3550/X	VMA672447	B\W	335
Recreation, Parks & Cultural Services	Equestrian Center	WorkCentre 6515	5AV812616	n/a	350
Public Safety	Public Safety Headquarters	WorkCentre 6605/DNM	XL3579711	n/a	350
Court	Municipal Court	Phaser 3610/DN	A4T020246	B\W	465



RFP 22-124, Managed Print Services

Record of Submissions

Supplier	Date Submitted	Confirmation Code
EDGE Business Systems	Jul 20, 2022 6:54 PM EDT	Mjl2NDE0
4ColorLaser	Jul 21, 2022 9:47 AM EDT	Mjl2NDU0



STAFF REPORT

Submitting Department: Legal

Submitted By: Lauren Shapiro

Sponsored By:

Meeting Date: September 26, 2022

I. AGENDA ITEM TITLE: FRAN SHOENTHAL MCQUEEN SETTLEMENT AGREEMENT

Approval of the Settlement Agreement and Full and Final Release of Claims by Fran Shoenthal McQueen and authorize the Mayor to execute all necessary documents.

II. RECOMMENDATION:

Approval of the Settlement Agreement and Full and Final Release of Claims by Fran Shoenthal McQueen and authorize the Mayor to execute all necessary documents.

III. BUDGET IMPLICATIONS:

BUDGETED ITEM: NO

FISCAL IMPACT: NO

INCLUDED IN CURRENT FY CPTL BUDGET: NO

INCLUDED IN CURRENT FY OPRT. BUDGET: NO

TOTAL PROJECT COST:

APPROPRIATIONS:

<u>ACCOUNT TITLE/NUMBER</u>	<u>DOLLAR AMOUNT</u>
-----------------------------	----------------------

EXTERNAL FUNDING SOURCES:

<u>ACCOUNT TITLE/NUMBER</u>	<u>DOLLAR AMOUNT</u>
-----------------------------	----------------------

IV. REPORT IN BRIEF:

V. ALTERNATIVES:

VI. ATTACHMENTS:

Settlement Agreement and Full and Final Release (McQueen), Settlement Agreement and Full and Final Release (McQueen Executed)

SETTLEMENT AGREEMENT AND FULL AND FINAL RELEASE OF CLAIMS

This Settlement Agreement and Full and Final Release of Claims (“Release” or the “Agreement”) is made by Fran Shoenthal McQueen (“McQueen”). “McQueen” as used herein shall be defined as Fran Shoenthal McQueen and her agents, attorneys, successors, executors, administrators, beneficiaries, heirs, assigns, insurers, and any persons who could make consortium claims.

As used herein, the term “Alpharetta Released Parties” shall collectively mean the following persons, bodies, and/or entities: City of Alpharetta, Georgia (“Alpharetta”); the Mayor of Alpharetta in his individual and official capacity; the City Council of Alpharetta (the “Alpharetta Council”), including all members of the Alpharetta Council in their respective individual and official capacities; Robert J. Regus, individually and in his former official capacity as City Administrator of Alpharetta, all officers, officials, agents, and/or employees of the Alpharetta Municipal Court in their respective individual and official capacities; all current or former elected or appointed officials of Alpharetta; Alpharetta’s directors, employees, servants, agents, officials, officers, elected and appointed persons, insurers and attorneys, in their official and individual capacities, together with their predecessors, successors and assigns, both jointly and severally.

As used herein, the term “Milton Released Parties” shall collectively mean the following persons, bodies, and/or entities: City of Milton, Georgia (“Milton”); the Mayor of Milton in his individual and official capacity; the City Council of Milton (the “Milton Council”), including all members of the Milton Council in their respective individual and official capacities; Steve Krokoff, individually and in his official capacity as City Manager of Milton; all officers, officials, agents, and/or employees of the Milton Municipal Court in their respective individual and official capacities; all current or former elected or appointed officials of Milton; Milton’s directors, employees, servants, agents, officials, officers, elected and appointed persons, insurers and attorneys, in their official and individual capacities, together with their predecessors, successors and assigns, both jointly and severally.

In full and final satisfaction of all claims, suits, costs, debts, demands, actions, and causes of action against the Alpharetta Released Parties and Milton Released Parties, and in consideration of the promises and covenants contained herein and the consideration set forth in Section 2 below, the adequacy and sufficiency thereof being hereby acknowledged, McQueen, the Alpharetta Released Parties, and the Milton Released Parties (collectively, the “Parties”) hereby agree as follows:

WHEREAS, the attorney for McQueen submitted correspondence to Alpharetta and Milton (collectively, the “Cities”) dated May 5, 2022 concerning potential claims/threatened litigation arising out of her appointment and work as Solicitor for the Cities, her classification while working as Solicitor for Alpharetta, and her not being selected to continue to work as Solicitor for the Cities in April 2022 (the “Claim Notice”). The Alpharetta Released Parties and Milton Released Parties have denied the allegations and claims identified in the Claim Notice and any and all other claims or

threatened claims that have been raised or could have been raised in the Claim Notice or that otherwise arise out of McQueen's appointment and work as Solicitor for the Cities;

WHEREAS, as of the date of this Agreement, McQueen has not filed any charge of discrimination against the Cities with the Equal Employment Opportunity Commission ("EEOC"), and the Cities would deny any allegations or charge of discrimination or unlawful conduct that McQueen has threatened to file with the EEOC against the Cities;

WHEREAS, the Parties wish to settle the disputed claims, allegations and contentions against the Alpharetta Released Parties and Milton Released Parties that have been made or that could have been made in the Claim Notice or that otherwise arise out of McQueen's appointment and work as Solicitor for the Cities, including but not limited to all claims, allegations and contentions that have been made or could be made in any future EEOC proceeding or lawsuit arising out of McQueen's appointment and work as Solicitor for the Cities, McQueen's classification while working as Solicitor for Alpharetta, and McQueen not being selected to continue to work as Solicitor for the Cities in April 2022, and any and all other known and unknown past claims, present claims or claims which otherwise might be asserted or could be asserted arising out of or from, or related to McQueen's appointment and work as Solicitor for the Cities (with any such existing or potential claims being more particularly described and set forth in the full and final release contained in Section 3 below), without the necessity of further expense, and without admission of liability on the part of the Alpharetta Released Parties and Milton Released Parties, which is expressly denied.

NOW THEREFORE, for and in consideration of the following covenants and obligations, and for such other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the Parties do hereby agree as follows:

1. Recitals and Introductory Paragraphs.

Each of the recitals set forth hereinabove, the introductory paragraphs above, and the defined terms contained therein, are hereby incorporated into and made a part of this Agreement, and the Parties to this Agreement hereby represent and warrant to the other that such recitals are true and correct.

2. Payment And Consideration.

A. At the express direction of McQueen's attorneys, and with McQueen's express approval, payment will be made by or on behalf of the Cities to the order of "Fran Shoenthal McQueen and her attorneys Schwartz Rollins, LLC" in the amount of ONE HUNDRED THOUSAND DOLLARS AND 00/100 (\$100,000.00) (the "Settlement Amount"). The Settlement Amount is allocated as consideration for the release and discharge of McQueen's claims and potential claims set forth in Section 3 below, the full and final settlement of any and all claims including attorney's fees against the Alpharetta Released Parties and Milton Released Parties set forth in Section 3 below, the covenant not to sue set forth in Section 7 below, the other

consideration set forth in subparagraph B. of this Section, and all other agreements and covenants contained herein. The Settlement Amount shall be delivered to the office of McQueen's attorneys within twenty-one (21) calendar days of the execution of the Agreement.

B. Other Consideration: (1) Upon any request for a work reference, the Cities will provide a neutral employment reference limited to McQueen's dates working for the Cities, positions held and pay rate; (2) McQueen agrees that she will not seek any employment with the Cities; (3) Nothing in this Agreement shall affect McQueen's ability to appear as a private attorney on behalf of a party in the Cities' Municipal Courts, subject to all local, state, and federal laws, rules, regulations, rights, and obligations that may be applicable to attorneys appearing as counsel in the Cities' Municipal Courts.

3. Full and Final Release.

For and in consideration of the consideration specified above and other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, McQueen does hereby knowingly and voluntarily release and forever discharge the Alpharetta Released Parties and Milton Released Parties from any and all known and unknown claims, allegations and contentions that have been made or that could have been made in the Claim Notice or that otherwise arise out of McQueen's appointment and work as Solicitor for the Cities, including but not limited to all claims, allegations and contentions that have been made or could be made in any future EEOC proceeding or lawsuit arising out of McQueen's appointment and work as Solicitor for the Cities, McQueen's classification while working as Solicitor for Alpharetta, and McQueen not being selected to continue to work as Solicitor for the Cities in April 2022, and any and all other known and unknown past claims, present claims or claims which otherwise might be asserted or could be asserted arising out of or from, or related to McQueen's appointment and work as Solicitor for the Cities (collectively, the "Released Claims").

The Released Claims that are the subject of this full and final release include all claims, actions, causes of action, damages, judgments, debts, liabilities, compensation, expenses, attorneys' fees, grievances, demands, appeals, requests for declaratory, injunctive or equitable relief, suits and proceedings of any kind and nature, whether based on any alleged tort (including but not limited to personal injury), statute, any contract or alleged contract, vicarious liability or other legal or equitable theory of recovery, whether for compensatory, treble, liquidated or punitive damages or other relief, whether at law or equity or otherwise, whether known or unknown, which McQueen ever had, now has or could have as of the effective date of this Agreement which are or may be based in whole or in part on, or due or may arise out of, or are or may be related to or with:

- (i) any claims that McQueen was not provided with due process, equal protection, freedom of speech, or freedom of association;
- (ii) any claims that McQueen was misclassified under any local, state, or federal law as

an independent contractor during any period of time or tenure during which she worked for Alpharetta as Solicitor or in any other Alpharetta Municipal Court position;

- (iii) deprivation of rights under the United States and/or Georgia Constitution, including, but not limited to, the First and/or Fourteenth Amendments possessed by McQueen individually or in a representative capacity;
- (iv) deprivation of civil, constitutional or equal rights under local, state or federal law including, but not limited to, 42 U.S.C. §§ 1981, 1983, 1985, 1986 and/or 1988; Title VII of the Civil Rights Act of 1964, as amended; the Equal Pay Act, the Civil Rights Act of 1991; the Employee Retirement Income Security Act (“ERISA”), the Americans with Disabilities Act; the Americans with Disabilities Amendments Act, the Rehabilitation Act of 1973; the Age Discrimination in Employment Act (“ADEA”), the Older Workers Benefit Protection Act; or otherwise;
- (v) retaliation, harassment (whether general harassment, sexual harassment or any other form or type of harassment), discrimination on the basis of age, gender, sex or any other protected characteristic or classification, failure to provide a workplace free of harassment, violence and/or retaliation, negligence, breach of policy and/or public policy, bad faith, hostile work environment, intentional or negligent infliction of emotional or mental distress, invasion of privacy/false light, including any alleged violations or non-compliance with the Health Insurance Portability and Accountability Act (“HIPAA”), outrageous conduct, negligent hiring or retention, failure to train, failure to warn, inducement, fraud, false imprisonment, assault, assault and battery, false arrest, malicious prosecution, breach of duty, libel, slander, defamation and/or tortious and/or criminal conduct of any kind;
- (vi) any claims of violation of or retaliation under O.C.G.A. § 45-1-4 (i.e., the Georgia Whistleblower Statute), or any claims of violation of or retaliation under any and all whistleblower protection statutes under federal law;
- (vii) interference with and/or breach of contract (express or implied, in fact or in law), detrimental reliance, breach of duty of good faith and fair dealing (express or implied) and/or breach of contract of any kind;
- (viii) tortious or negligent interference with business relationships, contractual relations or employment relationships of any kind, including any state law or federal claims alleging a foreclosure of opportunity for future employment;
- (ix) loss of consortium or society and companionship;
- (x) any alleged violation of, denial of rights, interference with rights, or retaliation

under the Family and Medical Leave Act of 1993, as amended (“FMLA”);

- (xi) any alleged violation of, denial of rights or retaliation under the Fair Labor Standards Act of 1938, as amended (“FLSA”), including any allegations of any unpaid overtime or claim of not being fully paid for hours of work performed while employed with or working for the Cities;
- (xii) attorneys’ fees, expenses or costs pursuant to 42 U.S.C. § 1988, 42 U.S.C. § 2000e-5(k) or as otherwise may be allowed by law, including pursuant to any state or federal statute, contract or common-law claim;
- (xiii) any and all other claims arising under law or equity;
- (xiv) denial of procedural or substantive due process;
- (xv) any alleged unlawful or ultra vires acts or conduct of any kind arising under or in reliance upon any statute, rules, regulations, laws, codes, and/or ordinances (whether federal, state or local); and
- (xvi) any and all other claims asserted or which could have been asserted by McQueen against the Alpharetta Released Parties and Milton Released Parties arising out of, from, by reason of, or that relate to McQueen’s employment with or work performed for the Cities.

Notwithstanding any other provision of this Section or of this Agreement, McQueen does not hereby waive any rights or claims for which waivers or releases are prohibited by applicable law or any rights or claims under the ADEA that may arise after the effective date of this Agreement, which for purposes of this Agreement shall be the day on which the Agreement is executed by McQueen.

4. Consultation With Attorney.

The Cities hereby advise McQueen in writing to consult with an attorney prior to executing this Agreement and waiver of claims under the ADEA.

5. Twenty-One Day Review Period Provided.

McQueen hereby acknowledges that, in accordance with federal law, she has been allowed up to twenty-one (21) days to consider whether to execute this Agreement and that she has had sufficient time to read and consider this Agreement before executing it. McQueen acknowledges that she has received valuable and good consideration to which McQueen is not otherwise entitled in exchange for her execution of this Agreement and executes this Agreement voluntarily, with a full understanding of its significance, and intending to be bound by its terms.

McQueen agrees that if she decides to shorten the 21-day period by executing this Agreement before the expiration of 21 days, she does so knowingly and voluntarily.

6. Seven-Day Revocation Period.

McQueen may revoke and cancel this Agreement at any time within seven (7) days after McQueen's execution of this Agreement by providing written notice to the Cities in the manner prescribed herein. If McQueen does so revoke, this Agreement will be null and void and the Cities shall have no obligation to provide any consideration to McQueen including, but not limited to that specified in Section 2 of this Agreement. This Agreement shall not become enforceable until after the expiration of the seven (7) day revocation period; after such time, if there has been no revocation, the Agreement shall be fully enforceable. In the event that McQueen chooses to revoke the Agreement, McQueen or her counsel shall notify the Cities by facsimile and e-mail to its designated agent for this purpose, Kenneth P. Robin, Jarrard & Davis, LLP, 222 Webb Street, Cumming, Georgia 30040, with the facsimile number (678) 455-7149 and the e-mail address of krobin@jarrard-davis.com, no later than 5:00 p.m. on the last day of the revocation period.

7. Covenant Not to Sue.

McQueen acknowledges and covenants that neither McQueen nor any other person, organization or other entity acting on McQueen's behalf has sued or will sue or cause or permit suit against the Alpharetta Released Parties and Milton Released Parties upon any of the Released Claims. McQueen further agrees that she will not directly or indirectly initiate, or cooperate or assist anyone else, with the initiation or advancement against the Cities of any notices, claims, lawsuits, actions, administrative proceedings or demands with the Internal Revenue Service or any other local, state or federal agency or authority that relate to or arise out of the Released Claims, including any existing or threatened claims pertaining to her classification during her tenure working for or being employed by the Cities.

8. No Other Claims and Covenants as to Classification and Compensation.

A. McQueen acknowledges and represents that she does not have any pending claims or charges against the Alpharetta Released Parties and Milton Released Parties. McQueen also acknowledges and represents that she will not file, or assign to others the right to file, or make claims or charges against the Alpharetta Released Parties and Milton Released Parties at any time for actions, representations, or omissions covered by the Full and Final Release provisions in Section 3 of this Agreement.

B. McQueen further covenants, acknowledges, and agrees that she was not misclassified with regard to her independent contractor status during the period of time she worked for Alpharetta as Solicitor or in any other Alpharetta Municipal Court position.

McQueen further acknowledges and represents that she has received all leave she may have been eligible for and that may have been required under the Family and Medical Leave Act of 1993, as amended (“FMLA”), and does not claim that the Cities violated or denied her rights under the FMLA. McQueen further acknowledges and represents that she was properly classified as to any work as Solicitor for the Cities under the Fair Labor Standards Act of 1938, as amended (“FLSA”), she has been fully paid (including any overtime to which she was entitled, if any) for work performed for the Cities, and does not claim that the Cities violated or denied her rights under the FLSA.

9. Return Of Property.

McQueen states that, in accordance with her existing and continuing obligations to the Cities, she has returned all property of the Cities, including, but not limited to, keys, files, records, maps, computer access codes, and computer programs, instruction manuals, business plans, and other property which McQueen maintained, prepared or helped to prepare in connection with her employment with or work as Solicitor for the Cities. In no event will McQueen remove any such items off the premises of the Cities, or duplicate any such items for removal from the premises of the Cities.

10. Cooperation.

McQueen agrees to fully cooperate with the Cities for a period of one year from the date of execution of this Agreement in any and all investigations, inquiries, or litigation in any judicial, administrative, or public, quasi-public, or private forum, in which the Cities are involved that relate directly to the manner in which she handled or oversaw any case that she has prosecuted on behalf of either of the Cities, whether or not McQueen is a party to or a subject of such investigations, inquiries, proceedings, or litigation. McQueen shall provide such testimony, background information, and other support and cooperation as the Cities may reasonably request. McQueen acknowledges, agrees, and covenants that she will not voluntarily disclose any information related to personnel, payroll, risk management, claims, insurance, or attorney-client privileged matters, or any other information related to her work as solicitor that is sensitive, private, and confidential, and received during the course and scope of her employment with or work for the Cities to any person or entity except the Cities or their designee. McQueen further agrees that she will not directly or indirectly cooperate or assist with the initiation or advancement of any claims, lawsuits, actions, administrative proceedings or demands against the Cities related to or arising out of the Released Claims on behalf of herself or any other individual, including but not limited to the initiation or advancement of any proceedings with the Internal Revenue Service or any other local, state or federal agency or authority. Nothing in this Paragraph shall prohibit McQueen from testifying truthfully pursuant to a subpoena in any legal proceeding in which the Cities are involved.

11. Sole and Entire Agreement.

It is expressly understood and agreed that this is a full, final and complete settlement and release of the Alpharetta Released Parties and Milton Released Parties as to and regarding the Released Claims, that all prior discussions and negotiations, whether written or oral, have no binding or legal effect and that the terms of this Agreement may not be altered, amended, modified or otherwise changed in any respect or particular manner whatsoever except by writing duly executed by McQueen and an authorized representative of the Cities.

12. Non-Admission of Liability or Wrongful Conduct.

The Agreement shall not be constituted as an admission of any liability, wrongdoing, retaliation, or discrimination, nor shall it be considered to be evidence of such liability, wrongdoing, retaliation, or discrimination by either Party to the Agreement, all of whom hereby affirmatively deny any wrongdoing. The Agreement shall not be any sort of admission against the interests of any of the Alpharetta Released Parties and Milton Released Parties by McQueen or any other person or entity, as the Alpharetta Released Parties and Milton Released Parties deny any and all allegations of wrongdoing that they have been accused of, and enter into this Agreement to save the time, trouble and expenses of litigation, and put this matter behind them once and for all.

13. No Assignment of Claims by McQueen.

McQueen further represents and warrants that no claims addressed by this Agreement have been assigned or transferred, expressly or impliedly by operation of law, to any other person or party and no person or parties are subrogated to the rights of McQueen in this matter and that all claims released herein are owned exclusively by McQueen, who has the authority to release them.

14. Affidavit Required By O.C.G.A. § 44-14-473

As further inducement to agreement to the payment and consideration set forth in this Agreement, McQueen hereby agrees, avers, and warrants, as a condition precedent to the settlement of this matter, that there are no hospital liens and no claims by any other person, firm, corporation, and/or any other entity against the consideration referred to herein related to or arising out of any medical care to McQueen. McQueen, who is a resident of Forsyth County in the State of Georgia, states that pursuant to O.C.G.A. § 44-14-473, all hospital bills incurred for treatment rendered to her have been fully paid or will be paid immediately upon receipt of the Settlement Amount of this compromise. This sworn statement shall constitute the affidavit required under O.C.G.A. § 44-14-473.

15. Waiver of Notice Required by O.C.G.A. § 33-24-41.2

McQueen hereby acknowledges that this settlement is in the amount of FIVE THOUSAND DOLLARS and 00/100 (\$5,000.00) or greater, and this acknowledgement waives the special notice

required under O.C.G.A. § 33-24-41.2 of the payment by an insurer or its representative to McQueen.

16. Severability.

If any Section, paragraph or part of this agreement is found void or unenforceable, the remainder of the Agreement shall not be affected by such a finding.

17. Advice of Counsel.

The undersigned have read this Agreement, and acknowledge that they have had the advice of counsel or have had the opportunity to consult with counsel and that no promise or representation of any kind, other than as contained herein, has been made by the Alpharetta Released Parties and Milton Released Parties or anyone acting for them.

18. Governing Law.

This Agreement shall be construed in accordance with the laws of the State of Georgia. Any dispute arising out of or in any way related to this Agreement shall be submitted to the Superior Court of Fulton County.

19. Acceptance as Complete Satisfaction of All Claims.

McQueen accepts the consideration set forth in this Agreement as full payment and complete satisfaction of the Released Claims.

20. Agreement, Construction and Interpretation.

The Parties hereto agree that, if an ambiguity or question of intent or interpretation arises, this Agreement is to be construed as if the Parties had drafted it jointly, as opposed to being construed against a party because it was responsible for drafting one or more provisions of the Agreement. As used in this Agreement, the plural includes the singular, and the singular includes the plural. Use of the plural, or the singular, as the case may be throughout this Agreement, shall be construed to give this Agreement a broader meaning and scope, rather than a narrower one.

21. Legally Binding Agreement.

McQueen understands and acknowledges that (A) this is a legally binding Agreement that includes a full and final release of claims; (B) that by signing this Agreement, she is hereafter barred from instituting the Released Claims against the Alpharetta Released Parties and Milton Released Parties in the manner and to the extent set forth herein; and (C) that this Agreement is final and binding.

22. Execution in Counterparts.

This Agreement may be executed in multiple counterparts, each of which shall be deemed an original and, together, shall constitute one and the same Agreement.

IN WITNESS WHEREOF, having carefully read this *Settlement Agreement and Full and Final Release of Claims* in its entirety and having fully informed herself of and understanding its contents, McQueen indicates her agreement and executes this Agreement of her own free will and accord and under seal by her signature as of this ____ day of _____, 2022.

Fran Shoenthal McQueen L.S. (Seal)

* * *

I HAVE READ AND APPROVED THIS SETTLEMENT AGREEMENT AND FULL AND FINAL RELEASE OF CLAIMS. FURTHER, I HEREBY ACKNOWLEDGE THAT I HAVE NO SEPARATE CLAIM FOR ATTORNEY'S FEES, COSTS, AND EXPENSES IN CONNECTION WITH THE PROSECUTION OF MY CLIENT'S RELEASED CLAIMS.

Debra Schwartz, Partner
Schwartz Rollins, LLC
Attorney for Fran Shoenthal McQueen

Acknowledged and Agreed to By:

CITY OF ALPHARETTA, GEORGIA

By: _____
Jim Gilvin, Mayor

Date: _____

Attested to By:

, City Clerk

Approved as to form:
JARRARD & DAVIS, LLP

Molly N. Esswein, City Attorney

Acknowledged and Agreed to By:

CITY OF MILTON, GEORGIA

By: _____
Peyton Jamison, Mayor

Date: _____

Attested to By:

City Clerk

Approved as to form:
JARRARD & DAVIS, LLP

Ken E. Jarrard, City Attorney

SETTLEMENT AGREEMENT AND FULL AND FINAL RELEASE OF CLAIMS

This Settlement Agreement and Full and Final Release of Claims ("Release" or the "Agreement") is made by Fran Shoenthal McQueen ("McQueen"). "McQueen" as used herein shall be defined as Fran Shoenthal McQueen and her agents, attorneys, successors, executors, administrators, beneficiaries, heirs, assigns, insurers, and any persons who could make consortium claims.

As used herein, the term "Alpharetta Released Parties" shall collectively mean the following persons, bodies, and/or entities: City of Alpharetta, Georgia ("Alpharetta"); the Mayor of Alpharetta in his individual and official capacity; the City Council of Alpharetta (the "Alpharetta Council"), including all members of the Alpharetta Council in their respective individual and official capacities; Robert J. Regus, individually and in his former official capacity as City Administrator of Alpharetta, all officers, officials, agents, and/or employees of the Alpharetta Municipal Court in their respective individual and official capacities; all current or former elected or appointed officials of Alpharetta; Alpharetta's directors, employees, servants, agents, officials, officers, elected and appointed persons, insurers and attorneys, in their official and individual capacities, together with their predecessors, successors and assigns, both jointly and severally.

As used herein, the term "Milton Released Parties" shall collectively mean the following persons, bodies, and/or entities: City of Milton, Georgia ("Milton"); the Mayor of Milton in his individual and official capacity; the City Council of Milton (the "Milton Council"), including all members of the Milton Council in their respective individual and official capacities; Steve Krokoff, individually and in his official capacity as City Manager of Milton; all officers, officials, agents, and/or employees of the Milton Municipal Court in their respective individual and official capacities; all current or former elected or appointed officials of Milton; Milton's directors, employees, servants, agents, officials, officers, elected and appointed persons, insurers and attorneys, in their official and individual capacities, together with their predecessors, successors and assigns, both jointly and severally.

In full and final satisfaction of all claims, suits, costs, debts, demands, actions, and causes of action against the Alpharetta Released Parties and Milton Released Parties, and in consideration of the promises and covenants contained herein and the consideration set forth in Section 2 below, the adequacy and sufficiency thereof being hereby acknowledged, McQueen, the Alpharetta Released Parties, and the Milton Released Parties (collectively, the "Parties") hereby agree as follows:

WHEREAS, the attorney for McQueen submitted correspondence to Alpharetta and Milton (collectively, the "Cities") dated May 5, 2022 concerning potential claims/threatened litigation arising out of her appointment and work as Solicitor for the Cities, her classification while working as Solicitor for Alpharetta, and her not being selected to continue to work as Solicitor for the Cities in April 2022 (the "Claim Notice"). The Alpharetta Released Parties and Milton Released Parties have denied the allegations and claims identified in the Claim Notice and any and all other claims or

threatened claims that have been raised or could have been raised in the Claim Notice or that otherwise arise out of McQueen's appointment and work as Solicitor for the Cities;

WHEREAS, as of the date of this Agreement, McQueen has not filed any charge of discrimination against the Cities with the Equal Employment Opportunity Commission ("EEOC"), and the Cities would deny any allegations or charge of discrimination or unlawful conduct that McQueen has threatened to file with the EEOC against the Cities;

WHEREAS, the Parties wish to settle the disputed claims, allegations and contentions against the Alpharetta Released Parties and Milton Released Parties that have been made or that could have been made in the Claim Notice or that otherwise arise out of McQueen's appointment and work as Solicitor for the Cities, including but not limited to all claims, allegations and contentions that have been made or could be made in any future EEOC proceeding or lawsuit arising out of McQueen's appointment and work as Solicitor for the Cities, McQueen's classification while working as Solicitor for Alpharetta, and McQueen not being selected to continue to work as Solicitor for the Cities in April 2022, and any and all other known and unknown past claims, present claims or claims which otherwise might be asserted or could be asserted arising out of or from, or related to McQueen's appointment and work as Solicitor for the Cities (with any such existing or potential claims being more particularly described and set forth in the full and final release contained in Section 3 below), without the necessity of further expense, and without admission of liability on the part of the Alpharetta Released Parties and Milton Released Parties, which is expressly denied.

NOW THEREFORE, for and in consideration of the following covenants and obligations, and for such other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the Parties do hereby agree as follows:

1. Recitals and Introductory Paragraphs.

Each of the recitals set forth hereinabove, the introductory paragraphs above, and the defined terms contained therein, are hereby incorporated into and made a part of this Agreement, and the Parties to this Agreement hereby represent and warrant to the other that such recitals are true and correct.

2. Payment And Consideration.

A. At the express direction of McQueen's attorneys, and with McQueen's express approval, payment will be made by or on behalf of the Cities to the order of "Fran Shoenthal McQueen and her attorneys Schwartz Rollins, LLC" in the amount of ONE HUNDRED THOUSAND DOLLARS AND 00/100 (\$100,000.00) (the "Settlement Amount"). The Settlement Amount is allocated as consideration for the release and discharge of McQueen's claims and potential claims set forth in Section 3 below, the full and final settlement of any and all claims including attorney's fees against the Alpharetta Released Parties and Milton Released Parties set forth in Section 3 below, the covenant not to sue set forth in Section 7 below, the other

consideration set forth in subparagraph B. of this Section, and all other agreements and covenants contained herein. The Settlement Amount shall be delivered to the office of McQueen's attorneys within twenty-one (21) calendar days of the execution of the Agreement.

B. Other Consideration: (1) Upon any request for a work reference, the Cities will provide a neutral employment reference limited to McQueen's dates working for the Cities, positions held and pay rate; (2) McQueen agrees that she will not seek any employment with the Cities; (3) Nothing in this Agreement shall affect McQueen's ability to appear as a private attorney on behalf of a party in the Cities' Municipal Courts, subject to all local, state, and federal laws, rules, regulations, rights, and obligations that may be applicable to attorneys appearing as counsel in the Cities' Municipal Courts.

3. Full and Final Release.

For and in consideration of the consideration specified above and other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, McQueen does hereby knowingly and voluntarily release and forever discharge the Alpharetta Released Parties and Milton Released Parties from any and all known and unknown claims, allegations and contentions that have been made or that could have been made in the Claim Notice or that otherwise arise out of McQueen's appointment and work as Solicitor for the Cities, including but not limited to all claims, allegations and contentions that have been made or could be made in any future EEOC proceeding or lawsuit arising out of McQueen's appointment and work as Solicitor for the Cities, McQueen's classification while working as Solicitor for Alpharetta, and McQueen not being selected to continue to work as Solicitor for the Cities in April 2022, and any and all other known and unknown past claims, present claims or claims which otherwise might be asserted or could be asserted arising out of or from, or related to McQueen's appointment and work as Solicitor for the Cities (collectively, the "Released Claims").

The Released Claims that are the subject of this full and final release include all claims, actions, causes of action, damages, judgments, debts, liabilities, compensation, expenses, attorneys' fees, grievances, demands, appeals, requests for declaratory, injunctive or equitable relief, suits and proceedings of any kind and nature, whether based on any alleged tort (including but not limited to personal injury), statute, any contract or alleged contract, vicarious liability or other legal or equitable theory of recovery, whether for compensatory, treble, liquidated or punitive damages or other relief, whether at law or equity or otherwise, whether known or unknown, which McQueen ever had, now has or could have as of the effective date of this Agreement which are or may be based in whole or in part on, or due or may arise out of, or are or may be related to or with:

- (i) any claims that McQueen was not provided with due process, equal protection, freedom of speech, or freedom of association;
- (ii) any claims that McQueen was misclassified under any local, state, or federal law as

an independent contractor during any period of time or tenure during which she worked for Alpharetta as Solicitor or in any other Alpharetta Municipal Court position;

- (iii) deprivation of rights under the United States and/or Georgia Constitution, including, but not limited to, the First and/or Fourteenth Amendments possessed by McQueen individually or in a representative capacity;
- (iv) deprivation of civil, constitutional or equal rights under local, state or federal law including, but not limited to, 42 U.S.C. §§ 1981, 1983, 1985, 1986 and/or 1988; Title VII of the Civil Rights Act of 1964, as amended; the Equal Pay Act, the Civil Rights Act of 1991; the Employee Retirement Income Security Act ("ERISA"), the Americans with Disabilities Act; the Americans with Disabilities Amendments Act, the Rehabilitation Act of 1973; the Age Discrimination in Employment Act ("ADEA"), the Older Workers Benefit Protection Act; or otherwise;
- (v) retaliation, harassment (whether general harassment, sexual harassment or any other form or type of harassment), discrimination on the basis of age, gender, sex or any other protected characteristic or classification, failure to provide a workplace free of harassment, violence and/or retaliation, negligence, breach of policy and/or public policy, bad faith, hostile work environment, intentional or negligent infliction of emotional or mental distress, invasion of privacy/false light, including any alleged violations or non-compliance with the Health Insurance Portability and Accountability Act ("HIPAA"), outrageous conduct, negligent hiring or retention, failure to train, failure to warn, inducement, fraud, false imprisonment, assault, assault and battery, false arrest, malicious prosecution, breach of duty, libel, slander, defamation and/or tortious and/or criminal conduct of any kind;
- (vi) any claims of violation of or retaliation under O.C.G.A. § 45-1-4 (i.e., the Georgia Whistleblower Statute), or any claims of violation of or retaliation under any and all whistleblower protection statutes under federal law;
- (vii) interference with and/or breach of contract (express or implied, in fact or in law), detrimental reliance, breach of duty of good faith and fair dealing (express or implied) and/or breach of contract of any kind;
- (viii) tortious or negligent interference with business relationships, contractual relations or employment relationships of any kind, including any state law or federal claims alleging a foreclosure of opportunity for future employment;
- (ix) loss of consortium or society and companionship;
- (x) any alleged violation of, denial of rights, interference with rights, or retaliation

under the Family and Medical Leave Act of 1993, as amended ("FMLA");

- (xi) any alleged violation of, denial of rights or retaliation under the Fair Labor Standards Act of 1938, as amended ("FLSA"), including any allegations of any unpaid overtime or claim of not being fully paid for hours of work performed while employed with or working for the Cities;
- (xii) attorneys' fees, expenses or costs pursuant to 42 U.S.C. § 1988, 42 U.S.C. § 2000e-5(k) or as otherwise may be allowed by law, including pursuant to any state or federal statute, contract or common-law claim;
- (xiii) any and all other claims arising under law or equity;
- (xiv) denial of procedural or substantive due process;
- (xv) any alleged unlawful or ultra vires acts or conduct of any kind arising under or in reliance upon any statute, rules, regulations, laws, codes, and/or ordinances (whether federal, state or local); and
- (xvi) any and all other claims asserted or which could have been asserted by McQueen against the Alpharetta Released Parties and Milton Released Parties arising out of, from, by reason of, or that relate to McQueen's employment with or work performed for the Cities.

Notwithstanding any other provision of this Section or of this Agreement, McQueen does not hereby waive any rights or claims for which waivers or releases are prohibited by applicable law or any rights or claims under the ADEA that may arise after the effective date of this Agreement, which for purposes of this Agreement shall be the day on which the Agreement is executed by McQueen.

4. Consultation With Attorney.

The Cities hereby advise McQueen in writing to consult with an attorney prior to executing this Agreement and waiver of claims under the ADEA.

5. Twenty-One Day Review Period Provided.

McQueen hereby acknowledges that, in accordance with federal law, she has been allowed up to twenty-one (21) days to consider whether to execute this Agreement and that she has had sufficient time to read and consider this Agreement before executing it. McQueen acknowledges that she has received valuable and good consideration to which McQueen is not otherwise entitled in exchange for her execution of this Agreement and executes this Agreement voluntarily, with a full understanding of its significance, and intending to be bound by its terms.

McQueen agrees that if she decides to shorten the 21-day period by executing this Agreement before the expiration of 21 days, she does so knowingly and voluntarily.

6. Seven-Day Revocation Period.

McQueen may revoke and cancel this Agreement at any time within seven (7) days after McQueen's execution of this Agreement by providing written notice to the Cities in the manner prescribed herein. If McQueen does so revoke, this Agreement will be null and void and the Cities shall have no obligation to provide any consideration to McQueen including, but not limited to that specified in Section 2 of this Agreement. This Agreement shall not become enforceable until after the expiration of the seven (7) day revocation period; after such time, if there has been no revocation, the Agreement shall be fully enforceable. In the event that McQueen chooses to revoke the Agreement, McQueen or her counsel shall notify the Cities by facsimile and e-mail to its designated agent for this purpose, Kenneth P. Robin, Jarrard & Davis, LLP, 222 Webb Street, Cumming, Georgia 30040, with the facsimile number (678) 455-7149 and the e-mail address of krobin@jarrard-davis.com, no later than 5:00 p.m. on the last day of the revocation period.

7. Covenant Not to Sue.

McQueen acknowledges and covenants that neither McQueen nor any other person, organization or other entity acting on McQueen's behalf has sued or will sue or cause or permit suit against the Alpharetta Released Parties and Milton Released Parties upon any of the Released Claims. McQueen further agrees that she will not directly or indirectly initiate, or cooperate or assist anyone else, with the initiation or advancement against the Cities of any notices, claims, lawsuits, actions, administrative proceedings or demands with the Internal Revenue Service or any other local, state or federal agency or authority that relate to or arise out of the Released Claims, including any existing or threatened claims pertaining to her classification during her tenure working for or being employed by the Cities.

8. No Other Claims and Covenants as to Classification and Compensation.

A. McQueen acknowledges and represents that she does not have any pending claims or charges against the Alpharetta Released Parties and Milton Released Parties. McQueen also acknowledges and represents that she will not file, or assign to others the right to file, or make claims or charges against the Alpharetta Released Parties and Milton Released Parties at any time for actions, representations, or omissions covered by the Full and Final Release provisions in Section 3 of this Agreement.

B. McQueen further covenants, acknowledges, and agrees that she was not misclassified with regard to her independent contractor status during the period of time she worked for Alpharetta as Solicitor or in any other Alpharetta Municipal Court position. McQueen further acknowledges and represents that she has received all leave she may have been

eligible for and that may have been required under the Family and Medical Leave Act of 1993, as amended ("FMLA"), and does not claim that the Cities violated or denied her rights under the FMLA. McQueen further acknowledges and represents that she was properly classified as to any work as Solicitor for the Cities under the Fair Labor Standards Act of 1938, as amended ("FLSA"), she has been fully paid (including any overtime to which she was entitled, if any) for work performed for the Cities, and does not claim that the Cities violated or denied her rights under the FLSA.

9. **Return Of Property.**

McQueen states that, in accordance with her existing and continuing obligations to the Cities, she has returned all property of the Cities, including, but not limited to, keys, files, records, maps, computer access codes, and computer programs, instruction manuals, business plans, and other property which McQueen maintained, prepared or helped to prepare in connection with her employment with or work as Solicitor for the Cities. In no event will McQueen remove any such items off the premises of the Cities, or duplicate any such items for removal from the premises of the Cities.

10. **Cooperation.**

McQueen agrees to fully cooperate with the Cities for a period of one year from the date of execution of this Agreement in any and all investigations, inquiries, or litigation in any judicial, administrative, or public, quasi-public, or private forum, in which the Cities are involved that relate directly to the manner in which she handled or oversaw any case that she has prosecuted on behalf of either of the Cities, whether or not McQueen is a party to or a subject of such investigations, inquiries, proceedings, or litigation. McQueen shall provide such testimony, background information, and other support and cooperation as the Cities may reasonably request. McQueen acknowledges, agrees, and covenants that she will not voluntarily disclose any information related to personnel, payroll, risk management, claims, insurance, or attorney-client privileged matters, or any other information related to her work as solicitor that is sensitive, private, and confidential, and received during the course and scope of her employment with or work for the Cities to any person or entity except the Cities or their designee. McQueen further agrees that she will not directly or indirectly cooperate or assist with the initiation or advancement of any claims, lawsuits, actions, administrative proceedings or demands against the Cities related to or arising out of the Released Claims on behalf of herself or any other individual, including but not limited to the initiation or advancement of any proceedings with the Internal Revenue Service or any other local, state or federal agency or authority. Nothing in this Paragraph shall prohibit McQueen from testifying truthfully pursuant to a subpoena in any legal proceeding in which the Cities are involved.

11. **Sole and Entire Agreement.**

It is expressly understood and agreed that this is a full, final and complete settlement and release of the Alpharetta Released Parties and Milton Released Parties as to and regarding the

Released Claims, that all prior discussions and negotiations, whether written or oral, have no binding or legal effect and that the terms of this Agreement may not be altered, amended, modified or otherwise changed in any respect or particular manner whatsoever except by writing duly executed by McQueen and an authorized representative of the Cities.

12. Non-Admission of Liability or Wrongful Conduct.

The Agreement shall not be constituted as an admission of any liability, wrongdoing, retaliation, or discrimination, nor shall it be considered to be evidence of such liability, wrongdoing, retaliation, or discrimination by either Party to the Agreement, all of whom hereby affirmatively deny any wrongdoing. The Agreement shall not be any sort of admission against the interests of any of the Alpharetta Released Parties and Milton Released Parties by McQueen or any other person or entity, as the Alpharetta Released Parties and Milton Released Parties deny any and all allegations of wrongdoing that they have been accused of, and enter into this Agreement to save the time, trouble and expenses of litigation, and put this matter behind them once and for all.

13. No Assignment of Claims by McQueen.

McQueen further represents and warrants that no claims addressed by this Agreement have been assigned or transferred, expressly or impliedly by operation of law, to any other person or party and no person or parties are subrogated to the rights of McQueen in this matter and that all claims released herein are owned exclusively by McQueen, who has the authority to release them.

14. Affidavit Required By O.C.G.A. § 44-14-473

As further inducement to agreement to the payment and consideration set forth in this Agreement, McQueen hereby agrees, avers, and warrants, as a condition precedent to the settlement of this matter, that there are no hospital liens and no claims by any other person, firm, corporation, and/or any other entity against the consideration referred to herein related to or arising out of any medical care to McQueen. McQueen, who is a resident of Forsyth County in the State of Georgia, states that pursuant to O.C.G.A. § 44-14-473, all hospital bills incurred for treatment rendered to her have been fully paid or will be paid immediately upon receipt of the Settlement Amount of this compromise. This sworn statement shall constitute the affidavit required under O.C.G.A. § 44-14-473.

15. Waiver of Notice Required by O.C.G.A. § 33-24-41.2

McQueen hereby acknowledges that this settlement is in the amount of FIVE THOUSAND DOLLARS and 00/100 (\$5,000.00) or greater, and this acknowledgement waives the special notice required under O.C.G.A. § 33-24-41.2 of the payment by an insurer or its representative to McQueen.

16. Severability.

If any Section, paragraph or part of this agreement is found void or unenforceable, the remainder of the Agreement shall not be affected by such a finding.

17. Advice of Counsel.

The undersigned have read this Agreement, and acknowledge that they have had the advice of counsel or have had the opportunity to consult with counsel and that no promise or representation of any kind, other than as contained herein, has been made by the Alpharetta Released Parties and Milton Released Parties or anyone acting for them.

18. Governing Law.

This Agreement shall be construed in accordance with the laws of the State of Georgia. Any dispute arising out of or in any way related to this Agreement shall be submitted to the Superior Court of Fulton County.

19. Acceptance as Complete Satisfaction of All Claims.

McQueen accepts the consideration set forth in this Agreement as full payment and complete satisfaction of the Released Claims.

20. Agreement, Construction and Interpretation.

The Parties hereto agree that, if an ambiguity or question of intent or interpretation arises, this Agreement is to be construed as if the Parties had drafted it jointly, as opposed to being construed against a party because it was responsible for drafting one or more provisions of the Agreement. As used in this Agreement, the plural includes the singular, and the singular includes the plural. Use of the plural, or the singular, as the case may be throughout this Agreement, shall be construed to give this Agreement a broader meaning and scope, rather than a narrower one.

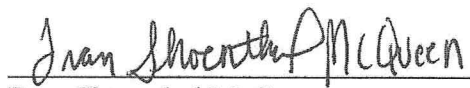
21. Legally Binding Agreement.

McQueen understands and acknowledges that (A) this is a legally binding Agreement that includes a full and final release of claims; (B) that by signing this Agreement, she is hereafter barred from instituting the Released Claims against the Alpharetta Released Parties and Milton Released Parties in the manner and to the extent set forth herein; and (C) that this Agreement is final and binding.

22. **Execution in Counterparts.**

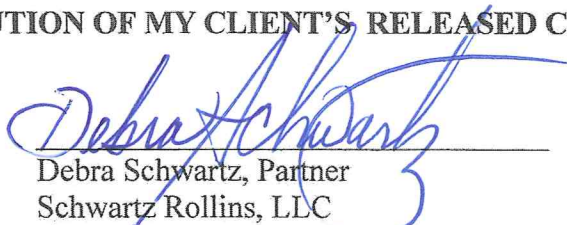
This Agreement may be executed in multiple counterparts, each of which shall be deemed an original and, together, shall constitute one and the same Agreement.

IN WITNESS WHEREOF, having carefully read this *Settlement Agreement and Full and Final Release of Claims* in its entirety and having fully informed herself of and understanding its contents, McQueen indicates her agreement and executes this Agreement of her own free will and accord and under seal by her signature as of this 20 day of September, 2022.

 L.S. (Seal)
Fran Shoenthal McQueen

* * *

I HAVE READ AND APPROVED THIS SETTLEMENT AGREEMENT AND FULL AND FINAL RELEASE OF CLAIMS. FURTHER, I HEREBY ACKNOWLEDGE THAT I HAVE NO SEPARATE CLAIM FOR ATTORNEY'S FEES, COSTS, AND EXPENSES IN CONNECTION WITH THE PROSECUTION OF MY CLIENT'S RELEASED CLAIMS.


Debra Schwartz, Partner
Schwartz Rollins, LLC
Attorney for Fran Shoenthal McQueen



STAFF REPORT

Submitting Department: Recreation, Parks & Cultural Services

Submitted By:

Sponsored By:

Meeting Date: September 26, 2022

I. AGENDA ITEM TITLE:

Playground Equipment Replacement: Webb Bridge Park (Webb Zone)

REMOVED: This item has been removed from the Consent Agenda by City Staff and will not be heard, discussed, or considered during tonight's meeting.

Approval of the purchase and installation of replacement playground equipment at Webb Bridge Park to Bliss Products & Services, Inc.

II. RECOMMENDATION:

III. BUDGET IMPLICATIONS:

BUDGETED ITEM: NO

FISCAL IMPACT: NO

INCLUDED IN CURRENT FY CPTL BUDGET: NO

INCLUDED IN CURRENT FY OPRT. BUDGET: NO

TOTAL PROJECT COST:

APPROPRIATIONS:

ACCOUNT TITLE/NUMBER	DOLLAR AMOUNT
----------------------	---------------

EXTERNAL FUNDING SOURCES:

ACCOUNT TITLE/NUMBER	DOLLAR AMOUNT
----------------------	---------------

IV. REPORT IN BRIEF:

V. ALTERNATIVES:

VI. ATTACHMENTS:



CITY COUNCIL MEETING STAFF REPORT

SUBMITTING DEPARTMENT: COMMUNITY DEVELOPMENT

SUBMITTED BY: KATHI COOK

DRAFTED BY: MICHAEL WOODMAN

I. AGENDA ITEM TITLE: Z-22-13/V-22-25 GRAND COMMUNITIES/2325 OLD MILTON PARKWAY

CITY COUNCIL: SEPTEMBER 26, 2022

This item was considered at the 9/1/2022 Planning Commission meeting. Staff recommended approval subject to 18 conditions. There was one (1) public comment in support of the proposal. After discussion, Planning Commission recommended approval subject to staff's recommended conditions and adding a condition addressing guest parking. Vote 7-0

II. RECOMMENDATION:

Approve Z-22-13/V-22-25 Grand Communities/2325 Old Milton Parkway, subject to the following conditions:

1. Approximately 6.15 acres shall be zoned DT-LW and developed substantially similar to site plan prepared by PEC, dated 4/19/22, except for modifications required to comply with the conditions below. However, lot yield depicted is not guaranteed and subject to meeting all City code requirements and conditions of zoning. The remaining 4 acres of the site shall remain in an undisturbed state.
2. Architecture and materials shall be developed substantially similar to the submitted renderings, labeled Exhibit A, except for modifications required to comply with the Downtown Consultant's comments and in compliance with the Alpharetta Downtown Code, subject to final approval by DRB. Townhomes shall have 4-sided architecture, materials and details. Townhome side elevation facing Old Milton Parkway shall have a porch or other significant projection to give the appearance as a front elevation, as approved by DRB.
3. Density shall not exceed 3.9 dwelling units per acre.
4. Courtyards may encroach into landscape strips, subject to meeting the minimum landscape material requirements, as approved by Staff.
5. Developer shall improve Old Milton Parkway streetscape with a minimum 4' planter planted with street trees (subject to Staff and GDOT approval), minimum 8' sidewalk, and decorative pedestrian lighting, with final approval by Staff. In lieu of tree grates, the soil area around street trees shall be planted with evergreen ornamental grasses, groundcovers and/or shrubs.
6. Streets, alleys and sidewalks internal to the site shall be developed as depicted on the site plan prepared by PEC, dated 4/19/22, with final approval by Staff. Decorative pedestrian lighting shall be required throughout the development. Internal streets and alleys shall be private and maintained by the HOA.
7. Minimum 10' landscape strip shall be required along both sides of internal streets, not including alleys. Landscape strips shall be exclusive of utilities and easements, except that if Fulton County requires an unencumbered easement shrubs shall replace tree requirements on one side of the street.
8. Minimum 20' landscape strip/building setback shall be provided along Old Milton Parkway. Landscape strip shall be planted with shade trees as a continuation of what has been planted or designed in the Downtown and outside of utility easements and overhead utilities, as approved by Staff.
9. A 20' planted buffer shall be provided as depicted on the site plan prepared by PEC, dated 4/19/22. A double row of evergreen and hardwood trees and shrubs shall be planted along the west property line adjacent to Units 1-4, as approved by Staff.
10. Project entrance shall include a decorative paver apron, landscaping, decorative low wall and/or fencing with columns, as approved by Staff.
11. Open space shall be developed substantially similar to the site plan prepared by PEC, dated 4/19/22, as approved by Staff. Open space shall be developed with a park-like setting with decorative landscape, hardscape and seating. Landscape shall include plant selections promoting the historic Downtown.
12. Creeping vines shall be planted to cover retaining and low walls, as approved by Staff.

13. Tree removal of specimen sized trees and trees of quality, as noted in the James Mahoney arborist report, shall be limited to trees in poor condition and tree #305, 323, 325, 1387, 1388, and 1389.
14. Fences and walls visible from the public right-of-way shall be decorative, as approved by Staff. Unfinished wood fences and decks shall not be visible from the street.
15. HVAC and similar equipment shall not be visible from the public right-of-way.
16. Garbage pickup shall be from within the development.
17. No more than 10% of the residential units shall be permitted to be rented, as recorded in the HOA's declarations and covenants.
18. To mitigate stream buffer impacts, developer shall comply with one or a combination of the following measures, as approved by Staff:
 - a. Provide 50% additional runoff reduction or water quality volume above the standard city requirements.
 - b. Provide buffer enhancement on an agreed upon area equal to at least 2 times the area of encroachment/impact. Enhancements may include removing fallen trees inside the stream bed that are impeding flow, plant eroded or sparsely vegetated areas of stream banks with live stakes, add enhanced buffer plantings where sparsely vegetated, and remove invasive vines.
 - c. Obtain any necessary state and federal approvals for the stream and buffer impacts.
 - d. Or alternative mitigation measures, as approved by Staff.
19. Minimum 4 guest parking spaces shall be provided on the site.

III. REPORT IN BRIEF:

The applicant, Grand Communities, LLC, is requesting a rezoning and variances to allow for the construction of twenty-four (24) 'For-Sale' townhomes on 6.15 acres in the Downtown. The proposed density is 3.9 dwelling units per acre. A rezoning is requested from R-12 (Dwelling, 'For-Sale', Residential) and O-I (Office-Institutional) to DT-LW (Downtown Live-Work). Variances are requested to allow up to twelve (12) townhomes to be front loaded, allow encroachments into a non-perennial stream buffer and impervious setback, and modify streetscape standards. The subject property is located at 2325 Old Milton Parkway, 0 Norcross Street, and 210 Norcross Street near the southeast corner of Old Milton Parkway and Haynes Bridge Road.

DISCUSSION

The submitted request, if approved, would allow for the construction of twenty-four (24) 'For-Sale' townhomes on 6.15 acres in the Downtown. The proposed density is 3.9 dwelling units per acre. The applicant proposes to rezone the property from R-12 (Dwelling, 'For-Sale', Residential) and O-I (Office-Institutional) to DT-LW (Downtown Live-Work). Variances are requested to allow up to twelve (12) townhomes to be front loaded, allow encroachments into a non-perennial stream buffer and impervious setback, and modify streetscape standards. The subject property is located at 2325 Old Milton Parkway, 0 Norcross Street, and 210 Norcross Street near the southeast corner of Old Milton Parkway and Haynes Bridge Road.

The undeveloped property is wooded and encumbered by approximately 3.1 acres of floodplain and stream buffers. Surrounding properties are zoned C-2 (General Commercial), DT-LW and O-I to the north, O-I and DT-LW to the east, R-4A (Dwelling, 'For-Sale', Attached Residential) to the south and R-4A, C-2 and O-I to the west. Haynes Park subdivision is located to the south and west, Alpharetta Crossing shopping center, My First Academy and Sabri Guven Fine Jewelry are located to the west, Beauty Facial Plastic Surgery and Chelsea Walk subdivision are located to the east, and undeveloped commercial properties are located to the north. The comprehensive land use plan designation of the property is 'Mixed Use Live Work', which allows the proposed use.

As shown in the table below, the applicant requests variances to modify Downtown Overlay site regulations (building orientation and streetscape standards) and Unified Development Code (UDC) regulations pertaining to a stream buffer encroachment. The property has an unusual shape, is situated between commercial properties, and has significant topography due to the presence of multiple streams and floodplain. The applicant proposes to mitigate the stream buffer and impervious setback encroachments (approximately 0.25 acres) by setting aside an

equivalent buffer and impervious setback area on the property. The set aside area for the new stream buffer and impervious setback should be outside of the 100-year floodplain.

Applicant's Variance Requests

UDC Section	Applicant's Request
Downtown Overlay – UDC Section 2.4.6(B)	Allow 12 townhomes to be front loaded
Downtown Overlay – UDC Section 2.3.3	Modify streetscape standards
UDC Section 3.3.2(D)(1)(a)	Allow encroachments into a non-perennial stream buffer (4,694 SF) and impervious setback (6,339 SF)

The table below identifies residential approvals in the Downtown since the adoption of the 2015 Downtown Master Plan update. The applicant's proposed density is lower than densities approved in the Downtown and along Old Milton Parkway.

Downtown – Residential Approvals since the 2015 Downtown Master Plan Update

Development Name	Type	Acres	Density
South of Wills Park	55 TH	5.5 acres	9.93 du/ac
236/244 North Main St	11 SFD	1.6 acres	6.8 du/ac
Mayfair on Main-217 South Main St	13 SFD, 11 TH	2.3 acres	10.4 du/ac
Hudson Park	16 SFD	2.41 acres	6.64 du/ac
The 1858	11 SFD	1.68 acres	6.55 du/ac
AlphaDev	11 SFD, 6 TH	2.21 acres	7.7 du/ac
Alcove Place	10 SFD	1.23 acres	8.1 du/ac
City Center/Voysey	42 SFD, 168 For-Rent	25 acres	8.0 du/ac
Midwick	17 SFD, 23 TH	5.85 acres	6.8 du/ac
Old Milton Holdings (Foundry)	25 SFD, 137 TH	23.89 acres	6.8 du/ac
Thompson Street Flats (Kairos)	24 Condo (High)	2.39 acres	10.0 du/ac
Burnett Circle (Ouray)	43 TH	5.72 acres	7.5 du/ac
Weyhill	9 SFD	3.1 acres	2.9 du/ac
Teasley Place	24 Condo (High)	1.5 acres	16 du/ac
East of Main	60 SFD, 42 TH	13.87 acres	7.35 du/ac
Twelve on Canton	12 SFD	5.46 acres	2.2 du/ac
The Maxwell	58 SFD, 80 Condo (Mid)	12.91 acres	10.7 du/ac
Rowes Downtown	22 SFD	3.26 acres	6.75 du/ac
Chelsea Walk	49 TH	7.04 acres	7.0 du/ac
Manning on the Square	58 SFD	11.7 acres	4.96 du/ac
Villa Magnolia	26 SFD	3.53 acres	7.37 du/ac
The Atley	86 TH/36 Condo (Mid)	15.3	7.97 du/ac

SITE PLAN

The submitted site plan depicts twenty-four (24), three (3) story 'For-Sale' townhomes with access from a new project entrance off Old Milton Parkway. Approximately four (4) acres of the property will remain undisturbed, including the property along Haynes Bridge Road. Most of the townhomes have access from a new private street, with eight (8) townhomes accessed from an alley. Half of the units will be rear loaded and half will be front loaded. Rear loaded units are twenty feet (20') wide and front-loaded units are 24' wide. Townhomes along Old Milton Parkway are setback approximately fifteen feet (15') from the right-of-way. Building setbacks comply with the DT-LW development standards; however, a twenty-foot (20') setback and landscape strip has been approved at other developments along Old Milton Parkway in the Downtown.

Five-foot (5') sidewalks are depicted along Old Milton Parkway and along the west side of the new internal private street. If approved, a minimum eight-foot (8') sidewalk should be provided along Old Milton Parkway. A twenty-foot (20') planted buffer is proposed adjacent to the medical office building to the east. A double row of evergreen trees and shrubs should be provided along the west property line adjacent to My First Academy daycare center.

Each townhome unit will have two (2) side-by-side parking spaces within a garage and a Code-compliant driveway accommodating two (2) additional cars. Two (2) guest parking spaces are provided near the mail kiosk. The Downtown Code requires 60 parking spaces for the proposed subdivision (2.5 parking spaces/unit), of which 98 spaces are provided on the site plan.

The site plan depicts 1.35 acres, or 22%, open space within the proposed development. The DT-LW district requires a minimum 10% amenity space and 10% civic space for properties over five (5) acres. Amenity space is proposed to include two (2) pocket parks, with one (1) located at the north end of the site and one (1) at the south end of the site. A mail kiosk is located near the southern pocket park and includes two (2) parking spaces. Civic space is noted to be a creek side greenway; however, improvements such as a trail are not depicted on the site plan.

Of the 24 specimen and trees of quality called out in the arborist report as fair condition or better, six (6) trees are proposed to be removed. Trees located in stream buffers and floodplain will be preserved, except in those areas where stream buffer encroachments have been requested. A stormwater management pond and bioretention area are depicted at the south end of the property adjacent to a pocket park.

RENDERINGS

The submitted elevations depict three (3) story townhomes in the Tudor Eclectic style, consisting primarily of brick with stone, board and batten and siding accents. Units will range in size from approximately 2,100 to 2,600 square feet and will be two (2) to four (4) bedrooms. According to the City’s Downtown Consultant, the proposed renderings generally comply with the design regulations in the Downtown Overlay.

TRAFFIC

The applicant provided a trip generation report (see table below), which estimates that the 24 townhome units would generate approximately seven (7) AM Peak Hour trips and ten (10) PM Peak Hour trips.

Table 1 – Trip Generation								
Land Use	Size	AM Peak Hour			PM Peak Hour			24 Hour
		Enter	Exit	Total	Enter	Exit	Total	Two-way
ITE 215 – Single-Family Attached Housing	24 units	2	5	7	5	5	10	132

SCHOOLS

Residential development is known to increase school enrollment. Fulton County calculated the potential maximum number of children who may live on the property by using the Fulton County Schools standard calculation to identify the number of children that a residential development will generate. The following chart outlines these figures:

FULTON COUNTY SCHOOLS – 24 Townhomes

School	Single Family Average #
Manning Oaks Elementary School	0 to 5 students
Northwestern Middle School	0 to 2 students
Milton High School	0 to 5 students
TOTAL	0 to 12 students

Based on the total figure for all three school levels, it can be assumed that the proposed development could house approximately 0 – 12 school age children. Numbers provided by Fulton County Schools show that Northwestern Middle School is approaching maximum capacity and Milton High School is over capacity.

STANDARDS FOR ZONING CHANGES

The Planning Commission and the City Council shall consider the following standards in considering a rezoning application, giving due weight or priority to those factors particularly appropriate to the circumstances of each application:

- a. Whether the zoning proposal will permit a use that is suitable in view of the zoning use and development of adjacent and nearby property.

Response: The proposed zoning is consistent with the future land use designation of the property and surrounding area, which is 'Mixed Use Live Work'. The area is envisioned to redevelop into a mix of residential, office and neighborhood commercial uses.

- b. Whether the zoning proposal will adversely affect the existing use or usability of adjacent or nearby property.

Response: The zoning proposal would not adversely affect the existing use or usability of adjacent or nearby properties. The area is envisioned to redevelop into a mix of residential, office and neighborhood commercial uses.

- c. Whether the zoning proposal will adversely affect the natural environment.

Response: The proposal should not have significant impacts on the natural environment. Approximately four (4) acres of the property will remain undeveloped. Tree saves are depicted on the applicant's site plan and mitigation is proposed to offset encroachments into the stream buffer and impervious setback.

- d. Whether there are substantial reasons why the property cannot or should not be used as currently zoned.

Response: The property is currently zoned R-12 and O-I, which have development regulations (setbacks) that are inconsistent with the Downtown vision to become a mixed-use, walkable environment. The requested zoning is consistent with the future land use designation of the property and surrounding area, which is 'Mixed Use Live Work'. The area is envisioned to redevelop into a mix of residential, office and neighborhood commercial uses.

- e. Whether the zoning proposal will result in a use that will or could cause an excessive or burdensome use of public facilities or services, including but not limited to existing streets and transportation facilities, schools, water or sewer utilities, and police or fire protection.

Response: The zoning proposal would not cause an excessive burden on public facilities and services. The requested rezoning to allow a residential development would increase demand on schools and parks; however, the proposed density is approximately half the average density approved in the Downtown.

f. Whether the zoning proposal is supported by new or changing conditions not anticipated or reflected in the existing zoning on the property.

Response: The subject property is located in the Downtown Overlay, which includes opportunities for properties to develop under the Downtown zoning districts. The requested zoning district is consistent with the future land use designation of the property and surrounding area, which is 'Mixed Use Live Work'.

g. Whether the zoning proposal reflects a reasonable balance between the promotion of the public health, safety, morality or general welfare against the right to unrestricted use of property.

Response: The request should not negatively impact public health, safety or welfare. The proposed zoning is consistent with the future land use designation of the property.

h. Whether there are substantial reasons why the property cannot be used in accordance with existing zoning.

Response: The property is currently zoned R-12 and O-I, which have development regulations (setbacks) that are inconsistent with the Downtown vision to become a mixed-use, walkable environment. The requested zoning is consistent with the future land use designation of the property and surrounding area, which is 'Mixed Use Live Work'. The area is envisioned to redevelop into a mix of residential, office and neighborhood commercial uses.

i. The extent to which the zoning proposal is consistent with the Comprehensive Plan.

Response: The future land use designation of the property is 'Mixed Use Live Work', which allows the proposed DT-LW zoning district, use and density.

VARIANCE REVIEW CRITERIA

The City of Alpharetta Unified Development Code Article IV, Section 4.5.3 outlines the criteria set forth for granting a variance. The ordinance specifically states..."a variance may be granted in whole or in part, or with conditions, in such individual case of unnecessary hardship upon a finding that":

(1) There are extraordinary and exceptional conditions pertaining to the particular piece of property in question because of its size, shape or topography; or

Response: The property has an unusual shape, has significant topographic challenges and is situated between multiple commercial properties, which are hardships that contribute to the requested variances. Approximately 3.1 acres of the property is encumbered by floodplain and stream buffers, of which the applicant requests to impact approximately 0.25 acres of impervious setback and stream buffer. Appropriate mitigation measures can be accommodated on the property.

(2) The application of the Ordinance to this particular piece of property would create an unnecessary hardship; or

Response: Application of the ordinance would create an unnecessary hardship given the unusual shape and significant topography on the property. Approximately 3.1 acres of the property is encumbered by floodplain and stream buffers, of which the applicant requests to impact approximately 0.25 acres of impervious setback and stream buffer. Appropriate mitigation measures can be accommodated on the property.

(3) There are conditions that are peculiar to the property which adversely affect its reasonable use or usability as currently zoned; or

Response: The property has significant topographic challenges and an unusual shape which contributes to the requested variances. Approximately 3.1 acres of the property is encumbered by floodplain and stream buffers, of which the applicant requests to impact approximately 0.25 acres of impervious setback and stream buffer. Appropriate mitigation measures can be accommodated on the property.

(4) Relief, if granted, would not cause substantial detriment to the public good or impair the purpose and intent of the City of Alpharetta ordinances.

Response: Relief, if granted, would not cause a substantial detriment to the public good. The applicant's proposed variances are related to hardships, including the unusual shape of the property and presence of topography. If approved, stream buffer encroachments should be mitigated with enhanced plantings and additional runoff reduction measures.

CONCURRENCES

Staff has reviewed the applicant's proposal against the established review criteria for a rezoning and variance. The zoning proposal is consistent with the vision of the Downtown Master Plan and future land use designation of the property. The proposed density of 3.9 dwelling units per acre is well below densities approved in the Downtown. If approved, the building setback and landscape strip along Old Milton Parkway should be a minimum twenty feet (20'), which is consistent with the setbacks and landscape strips approved at The Foundry, Wellstar, Northside Hospital, and One Alpharetta City office buildings.

There are exceptional conditions pertaining to the property due to its unusual shape, topography, presence of streams and floodplain, and location between commercial properties. Approximately 3.1 acres of the property is unbuildable due to the presence of streams and floodplain. It does not appear that variances are being requested for the purpose of increasing density. If approved, stream buffer encroachments should be mitigated with enhanced plantings and additional runoff reduction measures.

CITIZEN PARTICIPATION PLAN

The report submitted by the applicant states that property owners within 500' were contacted regarding the applicant's intent. The report states that no comments were received.

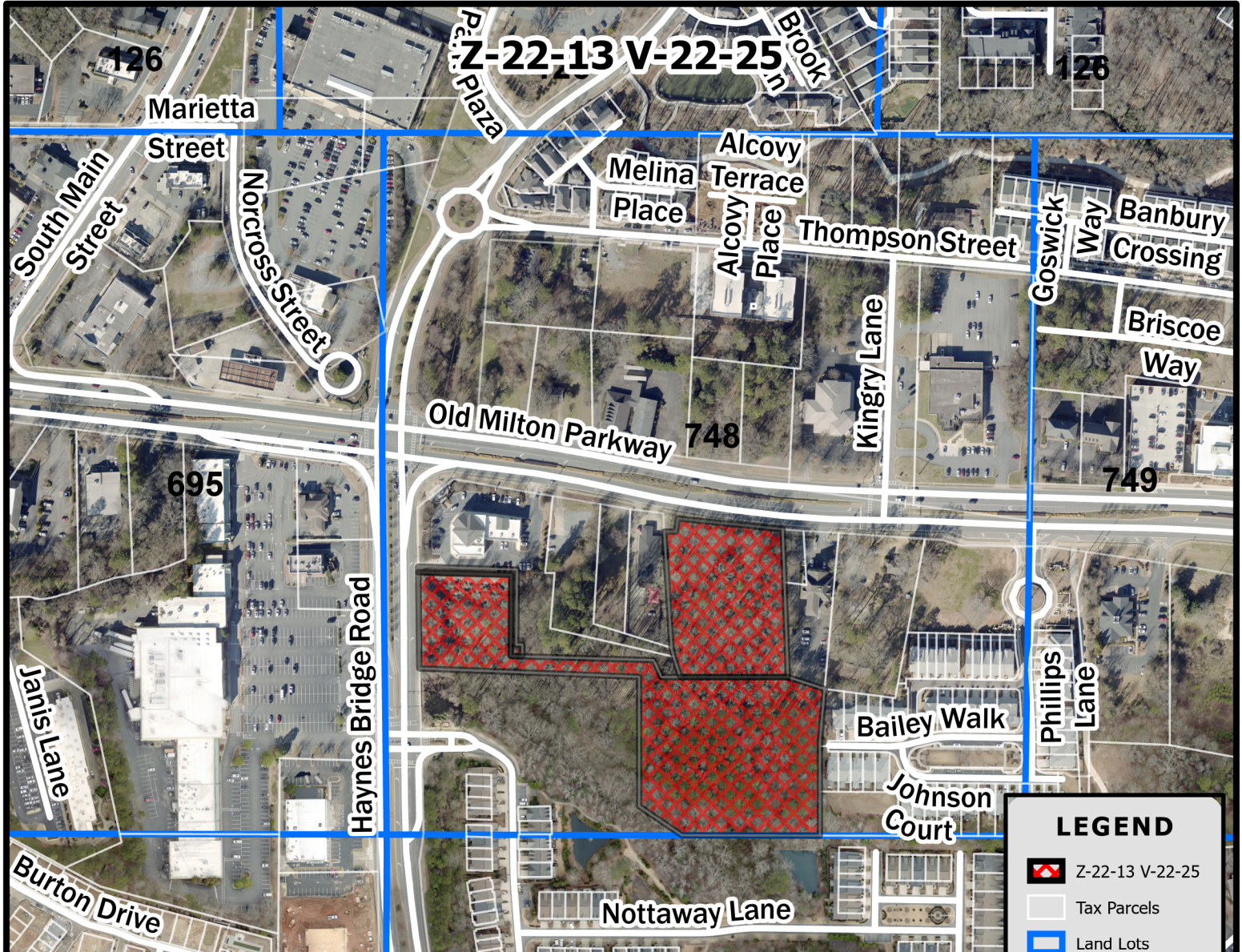
City Staff received correspondence from residents with concerns over flooding, habitat destruction, stream buffer impacts, proximity of detention pond to Chelsea Walk (buffers and potential for underground), and guest parking.

COMMUNITY ZONING INFORMATION MEETING

CZIM was held on August 10, 2022. There were public comments with concerns over sufficient guest parking, stream buffer encroachments and proximity of detention pond to Chelsea Walk.

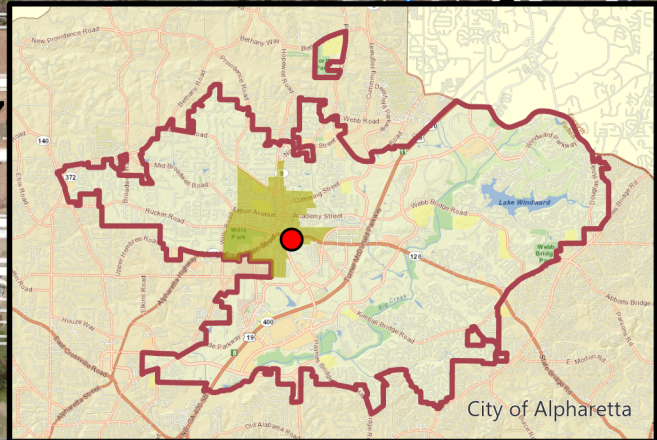
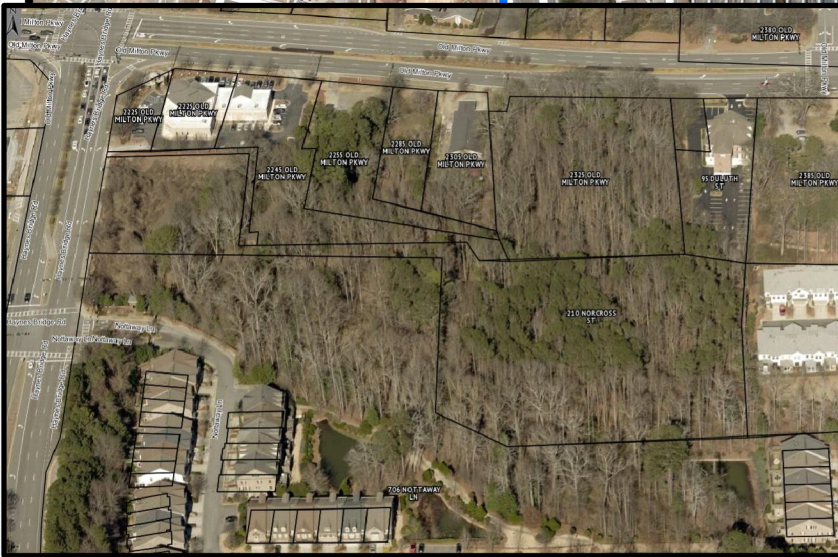
IV. ATTACHMENTS:

- Site Plan
- Renderings



LEGEND

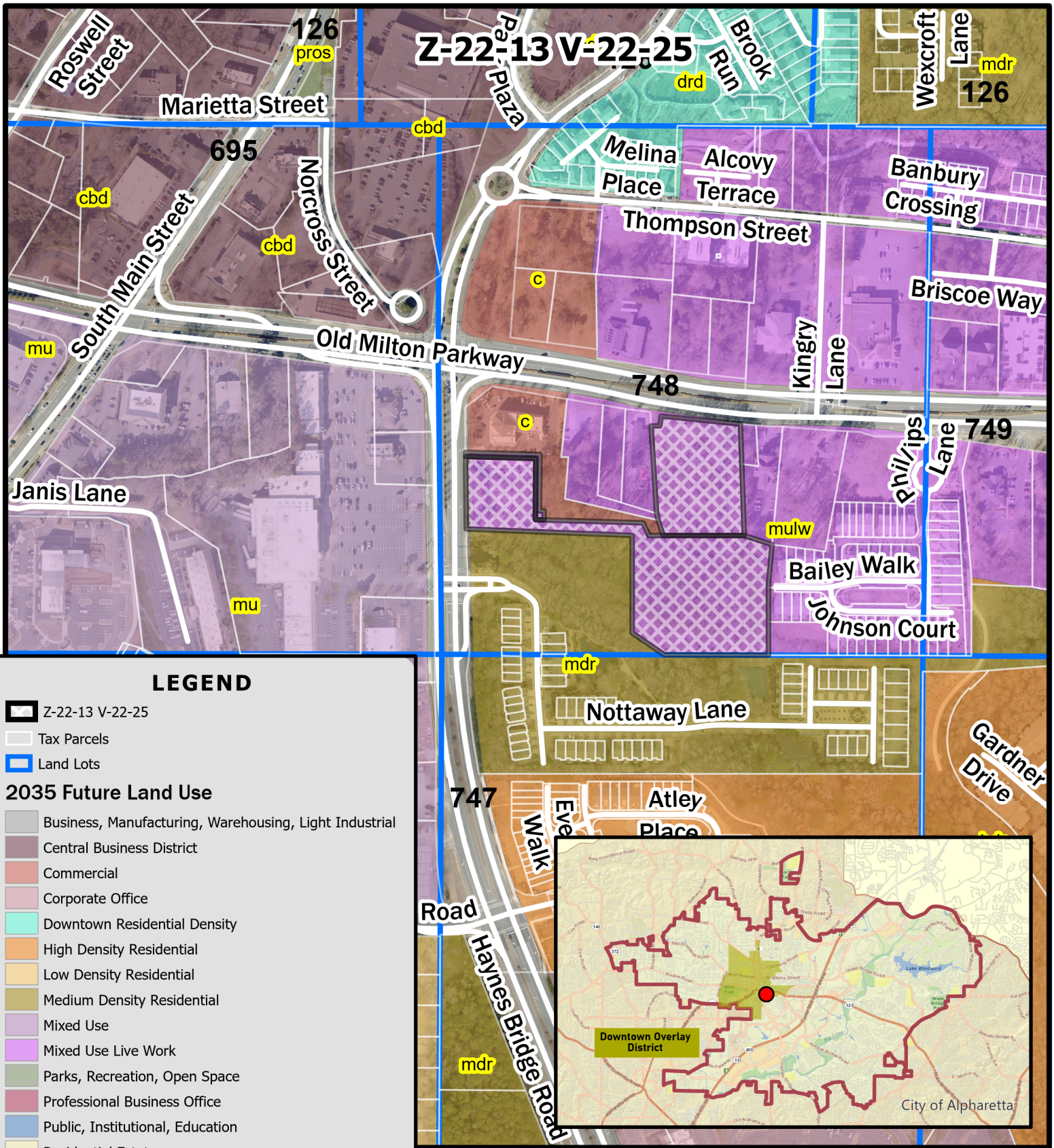
- Z-22-13 V-22-25
- Tax Parcels
- Land Lots



**Aerial Map
Fischer Homes
2325 Old Milton Parkway**

**Z-22-13 V-22-25
D/LL: 1/2/0748
PC: 9/01/22
CC: 9/26/22**

**Location Map Provided by:
Community Development - GIS**



LEGEND

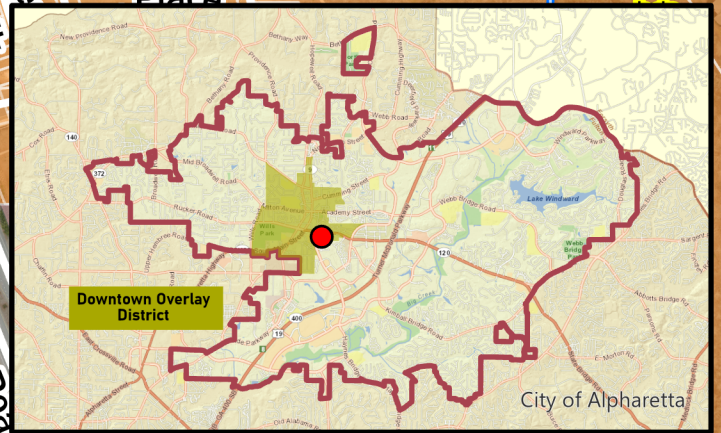
Z-22-13 V-22-25

Tax Parcels

Land Lots

2035 Future Land Use

- Business, Manufacturing, Warehousing, Light Industrial
- Central Business District
- Commercial
- Corporate Office
- Downtown Residential Density
- High Density Residential
- Low Density Residential
- Medium Density Residential
- Mixed Use
- Mixed Use Live Work
- Parks, Recreation, Open Space
- Professional Business Office
- Public, Institutional, Education
- Residential Estate
- Very Low Density Residential



Z-22-13 V-22-25

D/LL: 1/2/0748

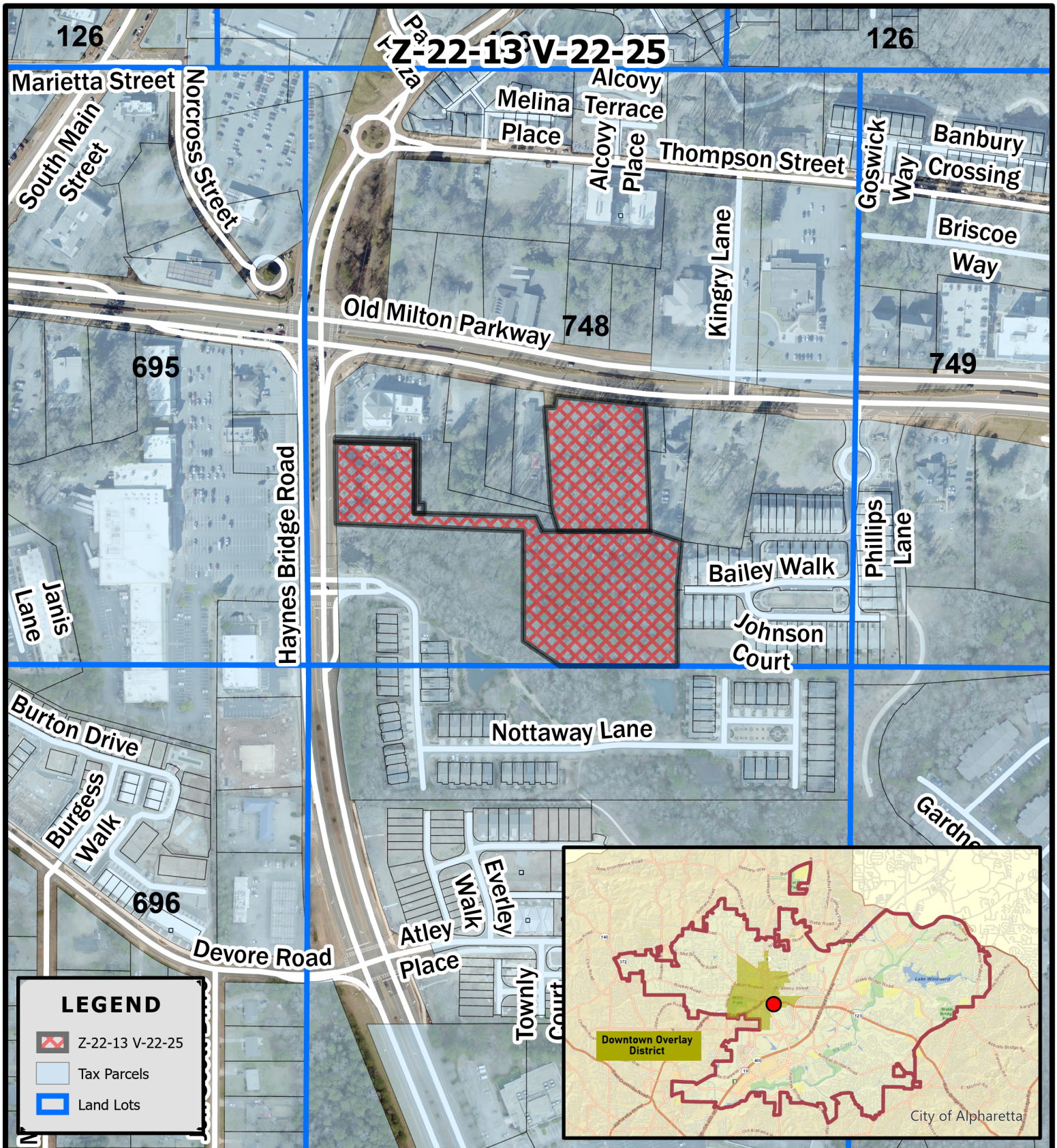
PC: 9/01/22

CC: 9/26/22



Future Land Use Map Fischer Homes 2325 Old Milton Parkway

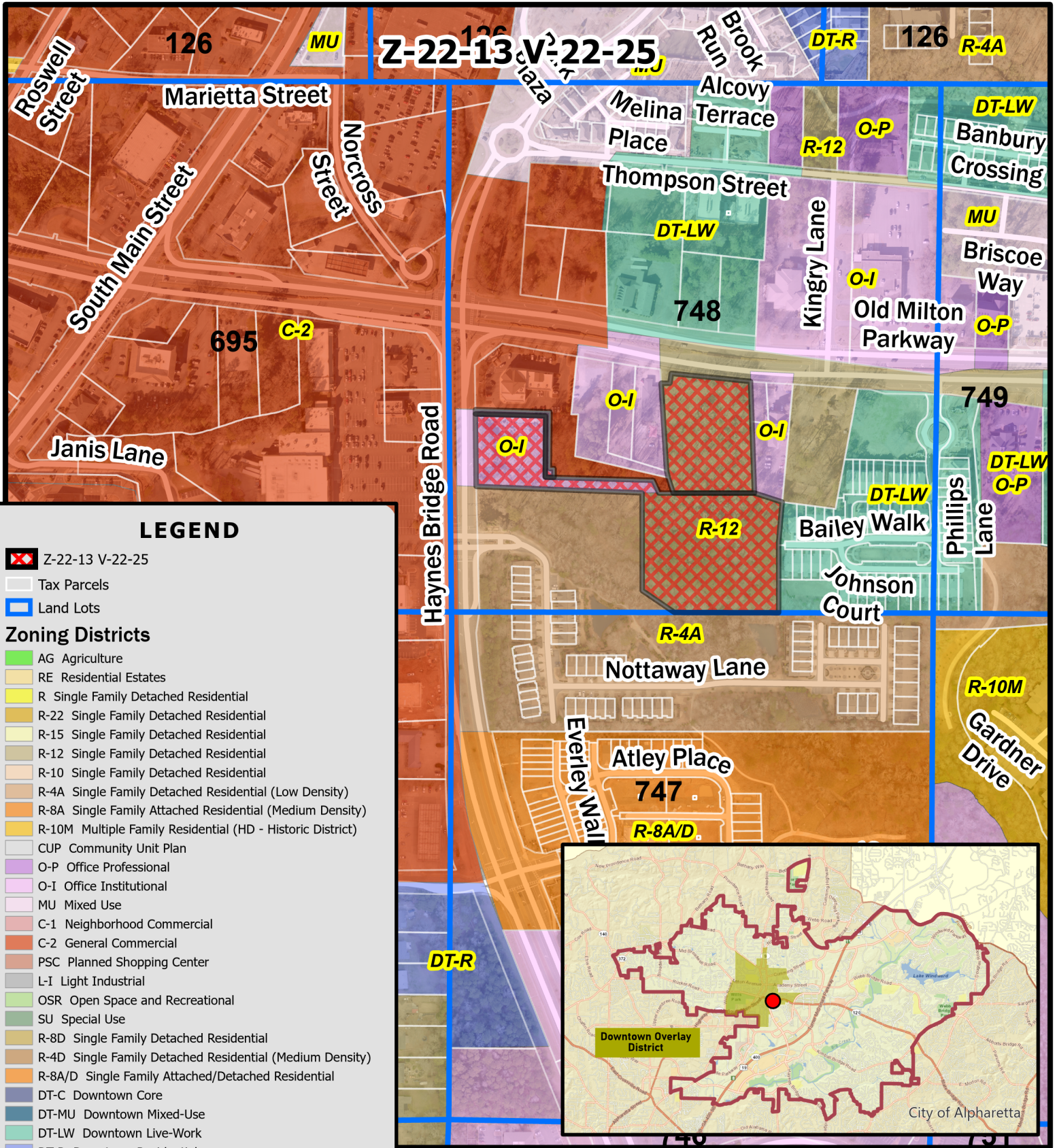
**Location Map Provided by:
Community Development - GIS**



Location Map **Fischer Homes** **2325 Old Milton Parkway**

Z-22-13 V-22-25
D/LL: 1/2/0748
PC: 9/01/22
CC: 9/26/22

Location Map Provided by:
Community Development - GIS



Zoning Map **Fischer Homes** **2325 Old Milton Parkway**

Z-22-13 V-22-25

D/LL: 1/2/0748

PC: 9/01/22

CC: 9/26/22

Location Map Provided by:
Community Development - GIS

FISCHER HOMES BACKGROUND

The Fischer Homes Legacy

- Privately held company
- Based in the Cincinnati Metropolitan area
- Founded in 1980 by Henry and Elaine Fischer
- 33,000 new homes constructed in 41 years
- Top 30 (by volume) US homebuilder in 2019
“Builder 100” list in Builder Magazine
- 15th largest private home builder
- Particular attention to neighborhood design
and architectural execution



“Dreams are meant to become reality.”

– Henry Fischer

FISCHER HOMES BACKGROUND

The Fischer Homes Legacy-Giving Back

- St. Jude's Research Hospital
 - > \$20 million raised through building 19 homes
 - Three homes in 2022: ~\$3.5 million raised in Cincinnati, Louisville and St. Louis
- Great American Ballpark "Nursing Suite"
(Baseball in Cincy)
 - Place for feeding/diapering young ones
- Family Care Center at Kings Island -2016
(Amusement park in Cincy)
 - Site for lost children, diaper changing/nursing area, cubbies/refrigerated storage



ALL LOCATIONS

Eight Divisions

- Northern Kentucky: Home base
- Atlanta, GA
- Cincinnati, OH
- Columbus, OH
- Dayton, OH
- Indianapolis, IN
- Louisville, KY
- St. Louis, MO





A hamlet in the heart of Downtown Alpharetta

- Cluster development
- Alpharetta as historic trading post location
- 24 market rate, fee simple lot, for-sale townhomes
- Walking distance to the downtown civic core and the Alpha loop trailhead on Old Milton Parkway



FISCHER HOMES MIDTOWN COLLECTION

Key Components

- Fee simple homesites – not condominiums
- Lifestyle living
 - HOA – low maintenance for owner
 - Discerning finishes
 - Lock and Leave
- Customization
 - Bed/bath combinations
 - Location of living/kitchen/dining
 - Finishes



FISCHER HOMES MIDTOWN COLLECTION

The Tustin

Key Features

- Primary building footprint: 20' x 44'-46' (at ground)
- 2-car attached garage, alley access
- 9' ceiling height
- 8' front door
- 3 bedrooms and 2.5 bathrooms included
- High level finishes: granite and quartz counter tops, upgraded interior trim, large shower tile in master bath, 42" kitchen wall cabinets, optional stacked wall cabinets, exterior use of brick and stone and fiber cement siding, composite decking with metal railings (interior and exterior).
- Outdoor living via rear balcony



FISCHER HOMES MIDTOWN COLLECTION

The Brookline

Key Features



Same as Tustin except:

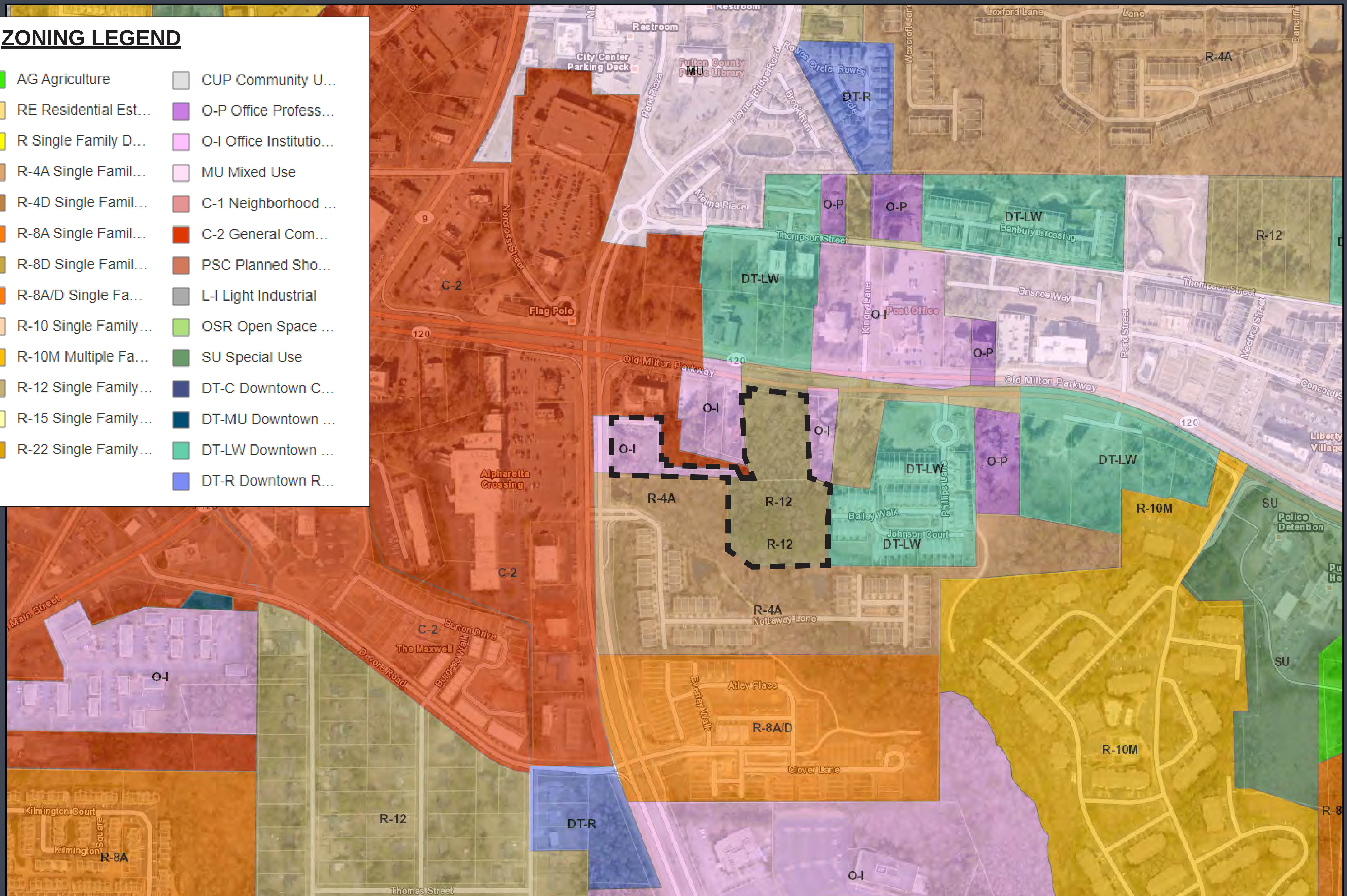
- Primary building footprint: 24' x 40'-42' (at ground level-wider because front entry garage)
- Outdoor living via rear yard and/or rear balcony (dependent upon topography)
- Larger square footage





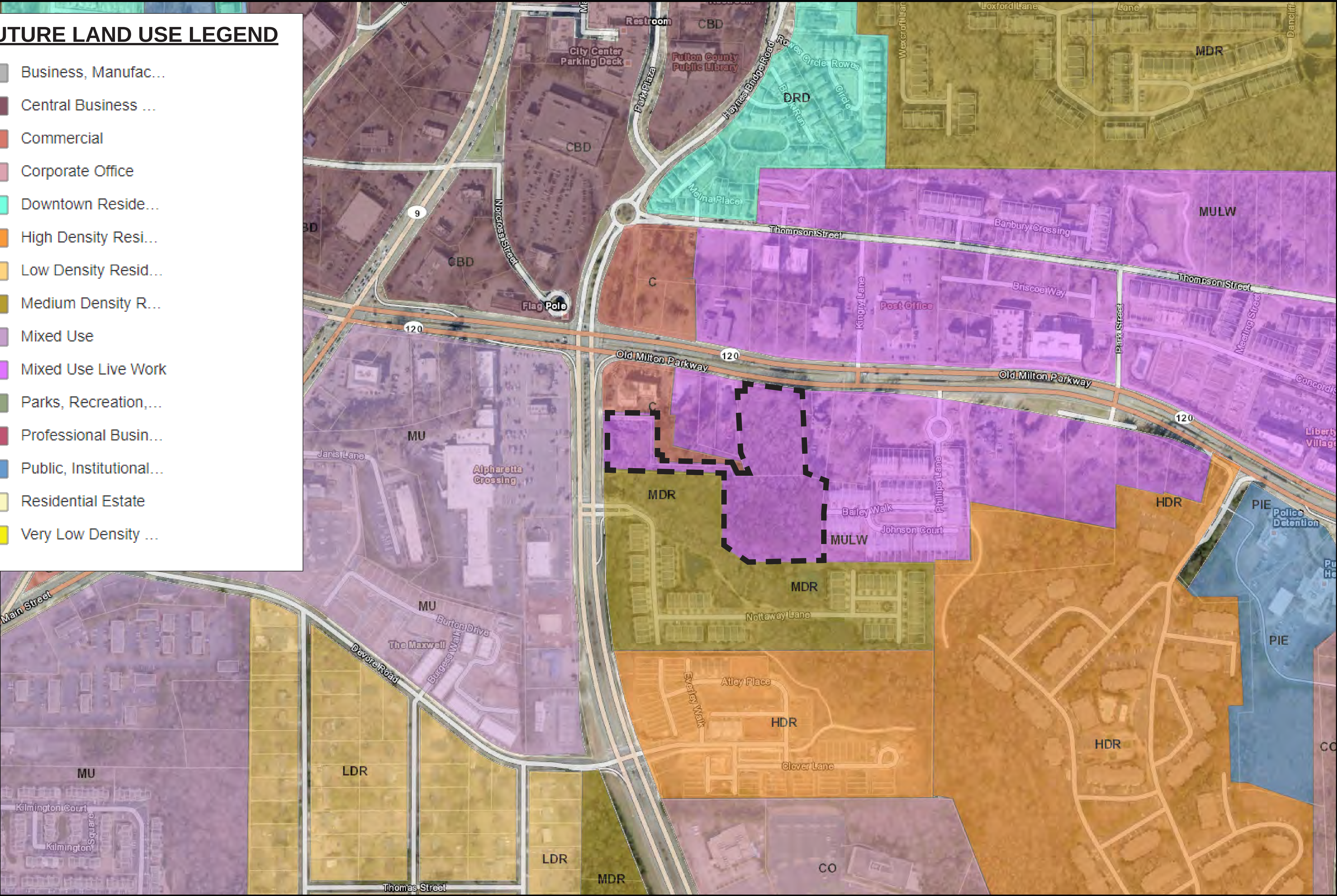
ZONING LEGEND

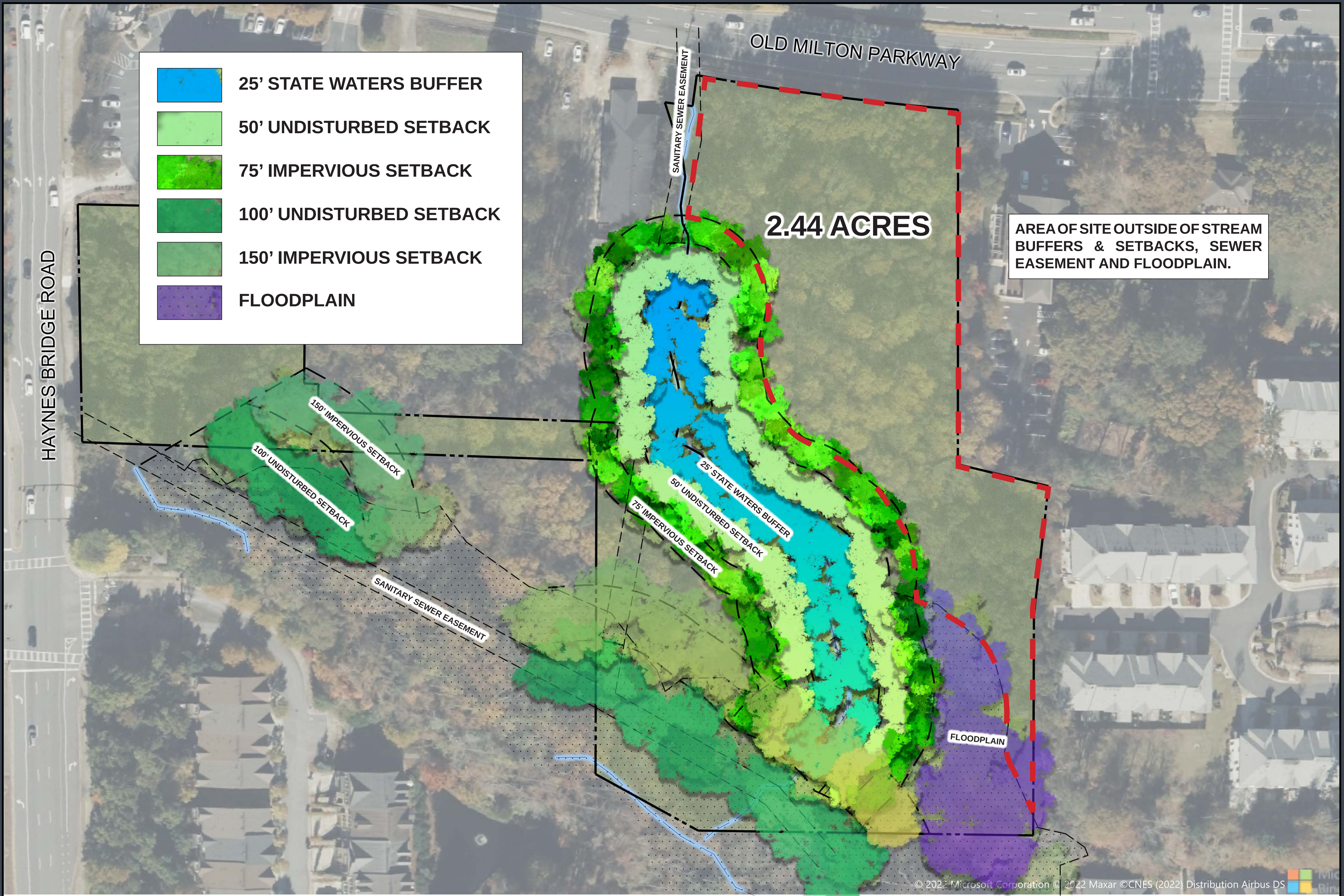
AG Agriculture	CUP Community U...
RE Residential Est...	O-P Office Profess...
R Single Family D...	O-I Office Institutio...
R-4A Single Famil...	MU Mixed Use
R-4D Single Famil...	C-1 Neighborhood ...
R-8A Single Famil...	C-2 General Com...
R-8D Single Famil...	PSC Planned Sho...
R-8A/D Single Fa...	L-I Light Industrial
R-10 Single Family...	OSR Open Space ...
R-10M Multiple Fa...	SU Special Use
R-12 Single Family...	DT-C Downtown C...
R-15 Single Family...	DT-MU Downtown ...
R-22 Single Family...	DT-LW Downtown ...
	DT-R Downtown R...



FUTURE LAND USE LEGEND

- Business, Manufac...
- Central Business ...
- Commercial
- Corporate Office
- Downtown Reside...
- High Density Resi...
- Low Density Resid...
- Medium Density R...
- Mixed Use
- Mixed Use Live Work
- Parks, Recreation,...
- Professional Busin...
- Public, Institutional...
- Residential Estate
- Very Low Density ...



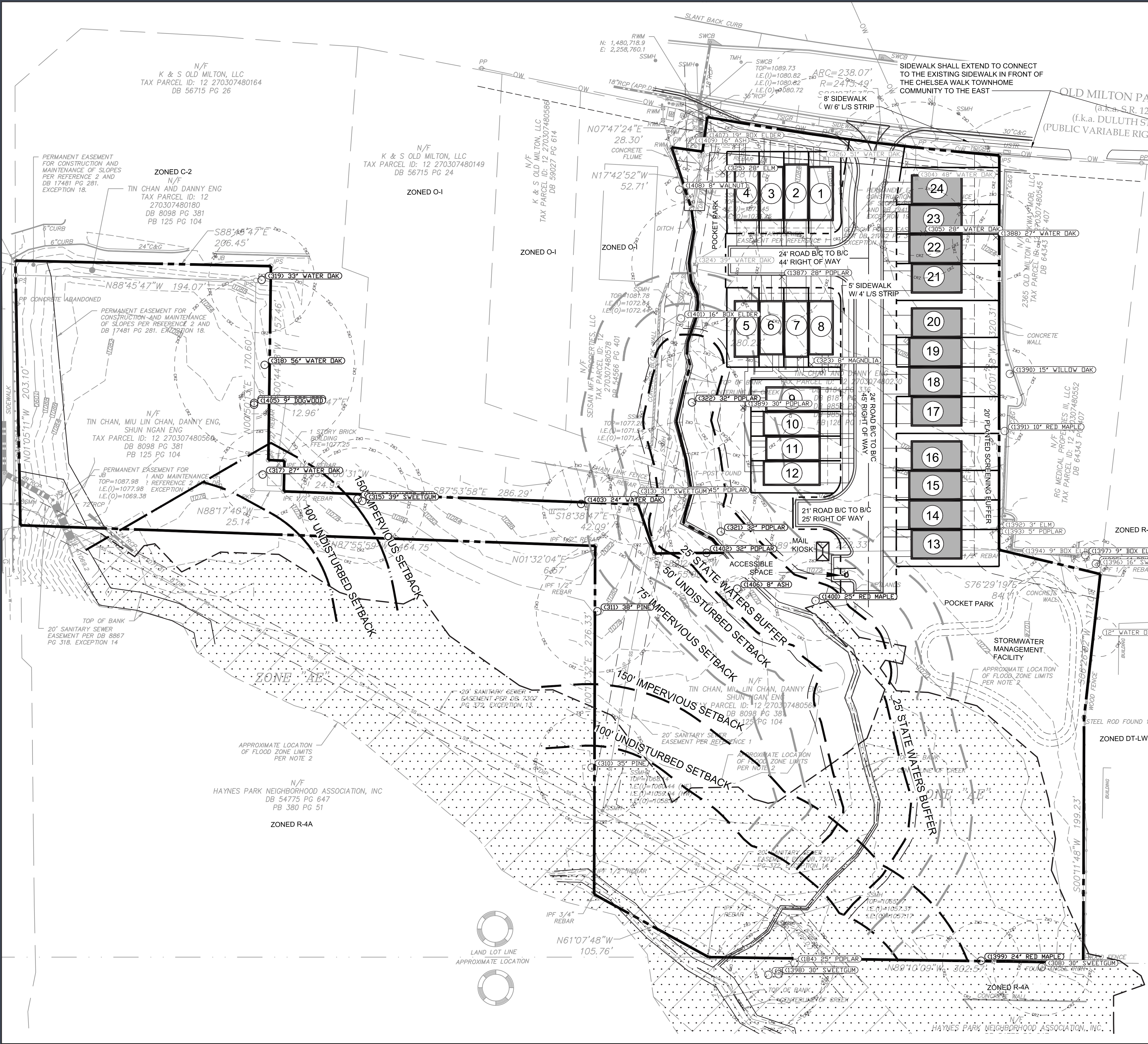




VARIANCES:

- 1) A STREAM BUFFER VARIANCE FOR THE DEVELOPMENT TO ENCROACH WITHIN THE UNDISTURBED AND IMPERVIOUS SETBACK.**
- 2) A VARIANCE FOR THE MODIFICATION OF STREETSCAPES; TO ALLOW INTERNAL SIDEWALK TO BE 5' WIDE WITH A 4' PLANTER STRIP INSTEAD OF THE REQUIRED 6' SIDEWALK AND 6' PLANTER STRIP.**
- 3) A VARIANCE FOR SOME TOWNHOMES TO BE FRONT-LOADED.**

SITE DATA:	
SITE AREA	±6.149 ACRES
ZONING	
EXISTING ZONING	R-12 (SFD 12,000 SF)/ O-I (OFFICE)
PROPOSED ZONING	DT-LW (DOWNTOWN LIVE-WORK)
OVERLAY DISTRICT	DOWNTOWN OVERLAY
ZONING JURISDICTION	CITY OF ALPHARETTA
USE CALCULATIONS	
MAXIMUM ALLOWABLE DENSITY	8 UNITS PER ACRE
PROPOSED 24' FRONT LOADED TOWNHOMES	12 UNITS
PROPOSED 20' REAR LOADED TOWNHOMES	12 UNITS
TOTAL PROPOSED DENSITY	24 UNITS (3.9 UPA)
SETBACK REQUIREMENTS	
FRONT SETBACK	10 FEET
SIDE SETBACK	0 FEET
REAR SETBACK	NO ALLEY- 3 FT; ALLEY- 10 FEET
DEVELOPMENT STANDARDS	
MAX BUILDING HEIGHT	40 FEET
PROPOSED MAX BUILDING HEIGHT	40 FEET
MAX LOT COVERAGE	70% (187,498.3 SF)
PROPOSED LOT OVERAGE	17% (45,520.5 SF)
MIN LOT SIZE	900 SF
PROPOSED MIN LOT SIZE	1,300 SF
MIN TOWNHOME WIDTH	20 FEET
PROPOSED MIN TOWNHOME WIDTH	20 FEET
MIN TOWNHOME SIZE	900 SF
PROPOSED MIN TOWNHOME SIZE	920 SF
OPEN SPACE CALCULATIONS	
CIVIC SPACE (POCKET PARKS)	27,392 SF (10.2%)
AMENITY SPACE (WOODED OPEN SPACE)	31,596 SF (11.7%)
PARKING REQUIREMENTS	
TOTAL PARKING REQUIRED	48 SPACES (RESIDENTIAL: 2 SPACES PER LOT)
PROPOSED RESIDENT PARKING	48 SPACES (2 SPACES PER GARAGE)
PROPOSED GUEST PARKING	50 SPACES
TOTAL PARKING PROVIDED	98 SPACES







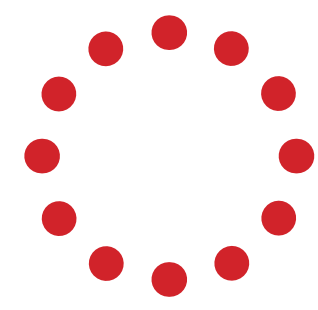




SPECIMEN TREES (FAIR OR BETTER QUALITY)



TREES TO REMAIN



TREES TO BE REMOVED



© 2022 Microsoft Corporation © 2022 Maxar ©CNES (2022) Distribution Airbus DS



CURRENT CONDITIONS



AFTER ENHANCEMENTS



•BANK REINFORCEMENT/STABILIZATION
(LIVESTAKES & VEGETATED GEOGRID)

•IMPROVED FILTRATION OF WATER

•STREAM BED CLEAN-UP

•REMOVAL OF INVASIVE SPECIES





LEFT SIDE / HIGH IMPACT ELEVATION



FRONT ELEVATION



COPYRIGHT ©2021 | FISCHER HOMES, INC. | ALL RIGHTS RESERVED.

THE TUSTIN | TUDOR ECLECTIC EXTERIOR

NOT FOR CONSTRUCTION



LEFT SIDE / HIGH IMPACT ELEVATION



FRONT ELEVATION



COPYRIGHT ©2021 | FISCHER HOMES, INC. | ALL RIGHTS RESERVED.

THE BROOKLINE | TUDOR ECLECTIC EXTERIOR

NOT FOR CONSTRUCTION



Entry Monument Concept for *'The Post'*

06.27.2022

COPYRIGHT ©2022 | FISCHER HOMES, INC. | ALL RIGHTS RESERVED.



THE POST

**DOWNTOWN
ALPHARETTA,
GEORGIA**

THANK YOU FOR YOUR TIME!

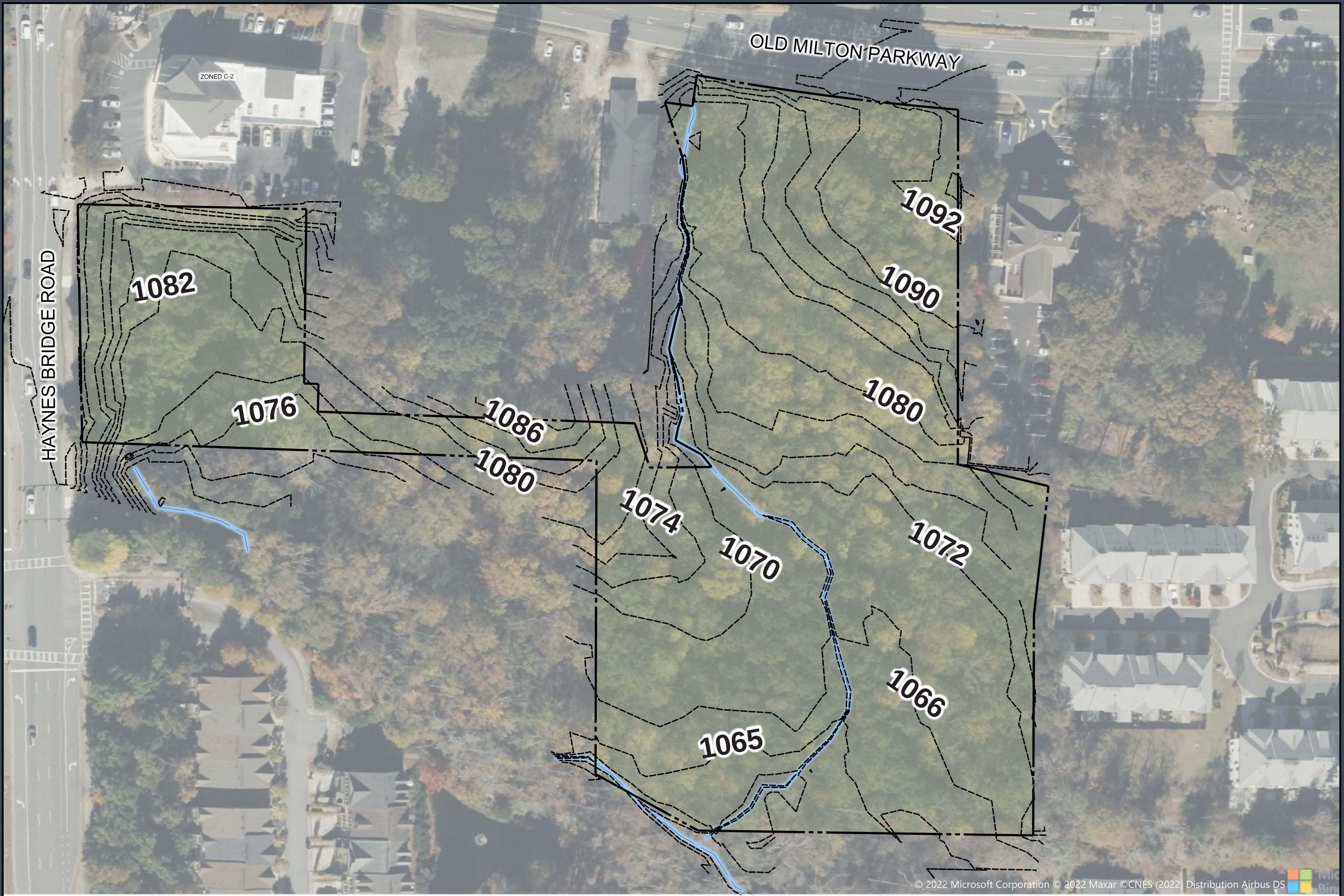
QUESTIONS?



2022

- 1 LANDSCAPED SEATING AREA
- 2 MULTI-PURPOSE FIELD
- 3 MULCH WALKING TRAIL
- 4 FIRE PIT







SITE LOCATION MAP

NOT TO SCALE

CIVIC SPACE - 0.62 ACRES
(10.1% OF OVERALL SITE)

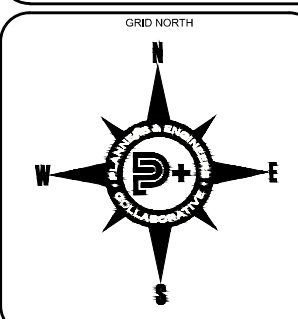
[illegible]

THIS SEAL IS ONLY VALID IF COUNTER SIGNED
AND DATED WITH AN ORIGINAL SIGNATURE.



GSWCC LEVEL II DESIGN PROFESSIONAL
CERTIFICATION # 0000059389 EXP. 10/28/2024

SCALE: 1" = 40'
DATE: 04/19/2022
PROJECT: 15315.01



E3

SHEET

24 HOUR CONTACT:
AMANDA WEBB



Know what's below.
Call before you dig.

CITIZEN PARTICIPATION FORM - PART B

This form must be completed and submitted to the City of Alpharetta Community Development Department a minimum of twenty (20) working days prior to the scheduled Public Hearing. Failure to do so will result in cancellation of the scheduled hearing.

Public Hearing or Project Name: Old Milton Parkway (The Post)

Contact Name: Ken Wood/Sonia Linton Telephone: 678-684-6256

Please describe comments and concerns provided by any and all individuals contacted as part of the the Citizen Participation Program. If any individuals provided written correspondence, please attach copies of same to this report.

Please find attached the Certification of Mailing from the USPS to show the letters were sent out to members of the public within 500 feet of the site. Since that time we have not received any emails or phone calls from these individuals with questions or concerns regarding the proposed development.

Method by which these individuals were contacted. Please mark all that apply. *Please provide samples of any and all written communications used to provide notification.*

- | | |
|--|--|
| ☒ Letter | ☐ Personal Visits |
| ☐ Telephone | ☐ Group Meeting |
| ☐ Email | ☐ Other <i>(Please Specify)</i> _____ |

Attach a list of people who have been notified of this application and provided information describing the subject proposal. Please note that ALL adjoining property owners MUST be notified.

I, the undersigned, as an authorized representative of the applicant and Public Hearing item identified above, do solemnly swear and attest, subject to criminal penalties for false swearing, that the information provided in this Citizen Participation Form - Part B and in any and all documents provided in support of this report are true and accurate. I further understand that any false statements provided by representatives of the applicant as part of this report may result in penalties up to and including denial of the subject application.

Signature of Authorized Agent: Sonia C. Linton

Digitally signed by Sonia C. Linton
DN: O="PEC+", CN=Sonia C. Linton, E=slinton@pec.plus
Reason: I am the author of this document
Location:
Date: 2022.08.04 11:44:08-04'00'
Foxit PDF Reader Version: 12.0.0

Date: 08/04/2022

Print Form

Community Zoning Information Meeting (CZIM)

August 10, 2022

Please sign-in and leave your comments and/or concerns.

Z-22-13/V-22-25 / Grand Communities/2325 Old Milton Parkway

NAME	ADDRESS	COMMENTS
ETT BOTT Hudsonhawk71@comcast.net	347 Bailey Walk Alpharetta GA	WHERE IS GUEST PARKING only showing 2 GUEST SPOTS.
Cheryl Batts Cheryl-Batts@icloud.com	347 Bailey Walk Alpharetta GA 30009	Concerns over Stream Buffer Reduction + Location of Detention Pond relative to Chelsea Walks + Inadequate Parking on site
Maureen Bruehly	716 Nottaway Lane Alpharetta, GA 30009	Please keep updated
Zhigang Xu	347 Bailey Walk mailing Address: 4575 Webb Bridge Rd #4002 Alpharetta, GA 30005 qbanexu@gmail.com	Please keep updates
Randall Morgan	604 Nottaway Lane Alpharetta 30009 ranjam1@gmail.com	

CITY OF ALPHARETTA

PUBLIC HEARING APPLICATION

FOR OFFICE USE ONLY

Case #: _____

PH #: _____

☐ Property Taxes & Code Violations Verified

☐ Fee Paid Initial: _____

COMMUNITY DEVELOPMENT DEPARTMENT

2 PARK PLAZA

ALPHARETTA, GA 30009

1. This page should be the first page in each of your completed application packets.
2. It is preferred that all responses be typed. Illegible applications will not be accepted.
3. Prior to signing and submitting your application, please check all information supplied on the following pages to ensure that all responses are complete and accurate. Incomplete applications will not be accepted.
4. Payment of all applicable fees must be made at the time of application. Payment may be made via cash, credit card (American Express, Master Card or Visa), or check made payable to "City of Alpharetta." Please note that a 3% convenience fee will be added to all credit card transactions.
5. Applications will be accepted on the designated submittal dates between the hours of 8:30 AM and 3:30 PM.
6. If you have any questions regarding this form, please contact the Community Development Department by calling 678-297-6070.

Contact Information:

Contact Name: Ken Wood; Sonia Linton Telephone: 678-684-6256

Address: 350 Research Court Suite: _____

City Peachtree Corners State: GA Zip: 30092 Fax: _____

Mobile Tel: 614-961-7630 Email: slinton@pec.plus

Subject Property Information:

Address: 235 Old Milton Parkway (0 & 210), Alpharetta, GA 30005 Current Zoning: R-12 & O-I

District: 12 Section: _____ Land Lot: 748 Parcel ID: 12 270307480230;12 270307480560;12 270307480180

Proposed Zoning: DT-LW Current Use: Undeveloped

This Application For (Check All That Apply):

☐ Conditional Use ☐ Master Plan Amendment ☐ Comprehensive Plan Amendment

☒ Rezoning ☐ Master Plan Review

☐ Variance ☐ Public Hearing

☐ Exception ☒ Other (Specify):

Stream Buffer Variance

APPLICANT REQUEST AND INTENT

What is the proposed use(s) of the property?

For the development of twenty-four (24) single-family attached townhomes on +/- 6.149 acres with a density of 3.9 du/acre.

Applicant's Request (Please itemize the proposal):

- To rezone the property from R-12 to DT-LW)
- To request a stream buffer variance to allow a portion of the site to encroach within the undisturbed and impervious setback.

Applicant's Intent *(Please describe what the proposal would facilitate).*

The applicant wishes to develop a little over 6 acres of property with 24 single-family attached townhomes. It proposes twelve 24-foot front loaded townhomes and twelve 20-foot rear loaded townhomes with an overall site density of 3.9 du/acre.

The majority of the site, about 4 acres, shall remain untouched due to the stream and wetlands to the south and west of the property.

A more detailed letter of intent has been included with the submittal package.

PROPERTY OWNER AUTHORIZATION

Property Owner Information:

Contact Name: **SEE ATTACHED** Telephone: _____

Address: _____ Suite: _____

City: _____ State: _____ Zip: _____ - _____

Authorization:

I do solemnly swear and attest, subject to criminal penalties for false swearing, that I am the legal owner, as reflected in the records of Fulton County, Georgia, of the property identified below, which is the subject of the attached Application for Public Hearing before the City of Alpharetta, Georgia.

As the legal owner of record of the subject property, I hereby authorize the individual named below to act as the applicant in the pursuit of the Application for Public Hearing in request of the items indicated below.

- | | |
|---|--|
| ☐ Annexation | ☐ Special Use |
| ☐ Rezoning | ☐ Conditional Use |
| ☐ Variance | ☐ Master Plan |
| ☐ Land Use Application | ☐ Other |

Property Owner's Authorized Applicant (if applicable):

Name of Authorized Applicant: _____ Telephone: _____

Address: _____ Suite: _____

City: _____ State: _____ Zip: _____ - _____

So Sworn and Attested:

Owner Signature: _____ Date: _____

Notary:

Notary Signature: _____ Date: _____

DISCLOSURE FORM

The Official Code of Georgia Annotated requires disclosure of campaign contributions to government officials by an applicant or opponent of a rezoning or public hearing petition (O.C.G.A. 36-67 A-1).

Applicants must file this form with the City of Alpharetta Community Development Department within ten (10) days after filing for rezoning or public hearing. Opponents to a rezoning or public hearing petition must file this form five (5) days prior to the Planning Commission meeting at which the subject rezoning or public hearing petition is scheduled to be heard.

Name of Applicant or Opponent: Ken Wood

Subject Public Hearing Case: 235 Old Milton Parkway

Campaign Contribution Information:

Please provide the requested information for each contribution with a dollar amount or value of \$250 or more made within the past two (2) years to an Alpharetta Official by the individual identified above. Please use a separate form for each Alpharetta Official to whom such a contribution has been made.

If the individual identified above has made no such contributions to an Alpharetta Official within the past two (2) years, please indicate this by entering "N/A" on the appropriate lines below.

Name of Official: N/A

Position: N/A

Description of Contribution: N/A

Value: N/A

Description of Contribution: _____

Value: _____

Description of Contribution: _____

Value: _____

Description of Contribution: _____

Value: _____

Description of Contribution: _____

Value: _____

Campaign Contribution Information:

I do solemnly swear and attest, subject to criminal penalties for false swearing, that the information provided in this Disclosure Form is true and accurate and that I have disclosed herein any and all campaign contributions made to an Official of the City of Alpharetta, Georgia in accordance with O.C.G.A. 36-67 A-3.

Signature: _____



Date: _____

6/28/2022

ALPHARETTA PLANNING COMMISSION REVIEW CRITERIA

How will this proposal be compatible with surrounding properties?

SEE ATTACHED

How will this proposal affect the use and value of the surrounding properties?

SEE ATTACHED

Can the property be developed for a reasonable economic use as currently zoned? Please explain why or why not.

SEE ATTACHED

What would be the increase to population and traffic if the proposal were approved?

SEE ATTACHED

What would be the impact to schools and utilities if the proposal were approved?

SEE ATTACHED

How is the proposal consistent with the Alpharetta Comprehensive Plan; particularly the Future Land Use Map?

SEE ATTACHED

Are there existing or changing conditions which affect the development of the property and support the proposed request?

SEE ATTACHED

On a separate sheet or sheets, please provide any information or evidence that supports your request and the statements that you have provided in this application.

CITIZEN PARTICIPATION FORM - PART A

This form must be completed and submitted with the applicant's completed Public Hearing Application. Applications submitted to the City of Alpharetta without a completed Citizen Participation Form - Part A will not be accepted.

Public Hearing or Project Name: Old Milton Parkway (The Post)

Contact Name: Ken Wood; Sonia Linton Telephone: 678-684-6256

The following people will be notified of this application and provided information describing the subject proposal. Please note that ALL adjoining property owners MUST be notified. Use additional pages as needed.

Seisan MFA Properties LLC

RG Medical Properties III LLC

K & S Old Milton LLC

Haynes Park Neighborhood Association Inc

JBL Atlanta Development LLC

MC Curdy L Tatum IV & MC Curdy Lawrence T

Edward & Cheryl Botts

Method by which these individuals will be contacted. Please mark all that apply. *If you select "Other," please provide a description of the method of contact that will be used.*

☒

Letter

☐

Personal Visits

☐

Telephone

☐

Group Meeting

☐

Email

☐

Other *(Please Specify)*

Please describe the method(s) by which these individuals will have the opportunity to respond or contact the applicant with questions or concerns about the proposal.

Contact email address and phone number will be provided in the letter for these individuals to reach out prior to and after the community meeting.

DETAILED TAX SUMMARY



City of Alpharetta

TAX YEAR: 2021 ▼

Owner Name

CHAN TIN & ENG DANNY

Parcel Identification

12 -2703-0748-018-0

Account Number

0696170

Property Location

0 NORCROSS STREET

Tax District

10 - ALPHARETTA

Fair Market Value

4,400

Assessed Value

1,760

Temporary Assessment

Not Found

City Exemption:

County Exemption:

<u>Levies</u>	<u>Assessment</u>	Exemptions	<u>Net Assessment</u>	X	<u>Net Rate</u>	<u>State Credit</u>	TAX
Fulton Cycle							
FULTON BONDS	1,760	0	1,760	X	.000210	\$0.00	\$0.37
FULTON OPER	1,760	0	1,760	X	.009330	\$0.00	\$16.42
FULTON SCHOOL GEN	1,760	0	1,760	X	.017590	\$0.00	\$30.96
INTEREST							\$0.00
PENALTIES/FEES							\$0.00
Last Payment: 10/15/2021			Total Amount Billed				\$47.75
			Less Amount Paid				\$47.75
			Total Due				\$0.00
City of Alpharetta Cycle							
INTEREST							\$0.00
PENALTIES/FEES							\$0.00
Last Payment: Not Found			Total Amount Billed				\$0.00
			Less Amount Paid				\$0.00
			Total Due				\$0.00

Property owners with current legal matters, such as bankruptcy or foreclosure, must contact the Tax Commissioner's office at (404) 613-6100 for the official balance due on their parcel(s).

[Return to Tax Bill](#) |

DETAILED TAX SUMMARY



City of Alpharetta

TAX YEAR: 2021 ▼

Owner Name

CHAN TIN & ENG DANNY

Parcel Identification

12 -2703-0748-023-0

Account Number

0696196

Property Location

2325 OLD MILTON PARKWAY

Tax District

10 - ALPHARETTA

Fair Market Value

200,000

Assessed Value

80,000

Temporary Assessment

Not Found

City Exemption:

County Exemption:

<u>Levies</u>	<u>Assessment</u>	Exemptions	<u>Net Assessment</u>	X	<u>Net Rate</u>	<u>State Credit</u>	TAX
Fulton Cycle							
FULTON BONDS	80,000	0	80,000	X	.000210	\$0.00	\$16.80
FULTON OPER	80,000	0	80,000	X	.009330	\$0.00	\$746.40
FULTON SCHOOL GEN	80,000	0	80,000	X	.017590	\$0.00	\$1,407.20
INTEREST							\$0.00
PENALTIES/FEES							\$0.00
Last Payment: 10/15/2021			Total Amount Billed				\$2,170.40
			Less Amount Paid				\$2,170.40
			Total Due				\$0.00
City of Alpharetta Cycle							
INTEREST							\$0.00
PENALTIES/FEES							\$0.00
Last Payment: Not Found			Total Amount Billed				\$0.00
			Less Amount Paid				\$0.00
			Total Due				\$0.00

Property owners with current legal matters, such as bankruptcy or foreclosure, must contact the Tax Commissioner's office at (404) 613-6100 for the official balance due on their parcel(s).

[Return to Tax Bill](#) |

DETAILED TAX SUMMARY



City of Alpharetta

TAX YEAR: 2021 ▼

Owner Name

CHAN TIN & ENG DANNY

Parcel Identification

12 -2703-0748-056-0

Account Number

0696323

Property Location

210 NORCROSS STREET

Tax District

10 - ALPHARETTA

Fair Market Value

473,600

Assessed Value

189,440

Temporary Assessment

Not Found

City Exemption:

County Exemption:

<u>Levies</u>	<u>Assessment</u>	Exemptions	<u>Net Assessment</u>	X	<u>Net Rate</u>	<u>State Credit</u>	TAX
Fulton Cycle							
FULTON BONDS	189,440	0	189,440	X	.000210	\$0.00	\$39.78
FULTON OPER	189,440	0	189,440	X	.009330	\$0.00	\$1,767.48
FULTON SCHOOL GEN	189,440	0	189,440	X	.017590	\$0.00	\$3,332.25
INTEREST							\$0.00
PENALTIES/FEES							\$0.00
Last Payment: 10/15/2021			Total Amount Billed				\$5,139.51
			Less Amount Paid				\$4,368.47
			Total Due				\$771.04
City of Alpharetta Cycle							
INTEREST							\$0.00
PENALTIES/FEES							\$0.00
Last Payment: Not Found			Total Amount Billed				\$0.00
			Less Amount Paid				\$0.00
			Total Due				\$0.00

Property owners with current legal matters, such as bankruptcy or foreclosure, must contact the Tax Commissioner's office at (404) 613-6100 for the official balance due on their parcel(s).

[Return to Tax Bill](#) |



The map shows the site location in the City of San Jose, California. The site is located at the intersection of Highway 101 and Highway 88, near the intersection of Highway 101 and Highway 88. The map includes labels for various streets and landmarks, such as the San Jose City Center, the San Jose City Hall, and the San Jose City Library. The site is highlighted in red.

SITE LOCATION MAP

NOT TO SCALE

GENERAL NOTES:

1. STREAM BUFFER VARIANCE REQUEST FOR DEVELOPMENT TO ENCOACH WITHIN THE UNDISTURBED AND IMPERVIOUS SETBACK. A MITIGATION PLAN HAS BEEN INCLUDED WITHIN THE REZONING SUBMITTAL.
2. ENTIRE SITE IS WOODED. FOR A MORE DETAILED VIEW OF SIGNIFICANT TREES WITH CRITICAL ROOT ZONES, SEE ARBORIST REPORT INCLUDED WITHIN REZONING SUBMITTAL.

GEORGIA811
www.Georgia811.com

Know what's below.
Call before you dig.



Planners & Engineers Collaborative+

LAND PLANNING + LANDSCAPE ARCHITECTURE + CIVIL ENGINEERING
ARBORISTS + SURVEYING & CONSTRUCTION + WATER RESOURCES

350 RESEARCH COURT STE 200
PEACHTREE CORNERS, GA 30092

PROJECT

2325 OLD MILTON

A MASTER PLANNED RESIDENTIAL
DEVELOPMENT

AT

2325 OLD MILTON
NORCROSS STREET
HAYNES BRIDGE ROAD

**CITY OF ALPHARETTA
JURISDICTION**

FOR

GRAND COMMUNITIES, LLC

MUNICIPALITY PROJECT #

REVISIONS

[illegible]

THIS SEAL IS ONLY VALID IF COUNTER SIGNED
AND DATED WITH AN ORIGINAL SIGNATURE.

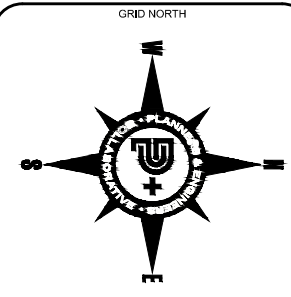


GSWCC LEVEL II DESIGN PROFESSIONAL
CERTIFICATION # 0000059389 EXP. 10/28/2024

ZONING SITE PLAN



SCALE: 1" = 40'
DATE: 04/19/2022
PROJECT: 15315.01

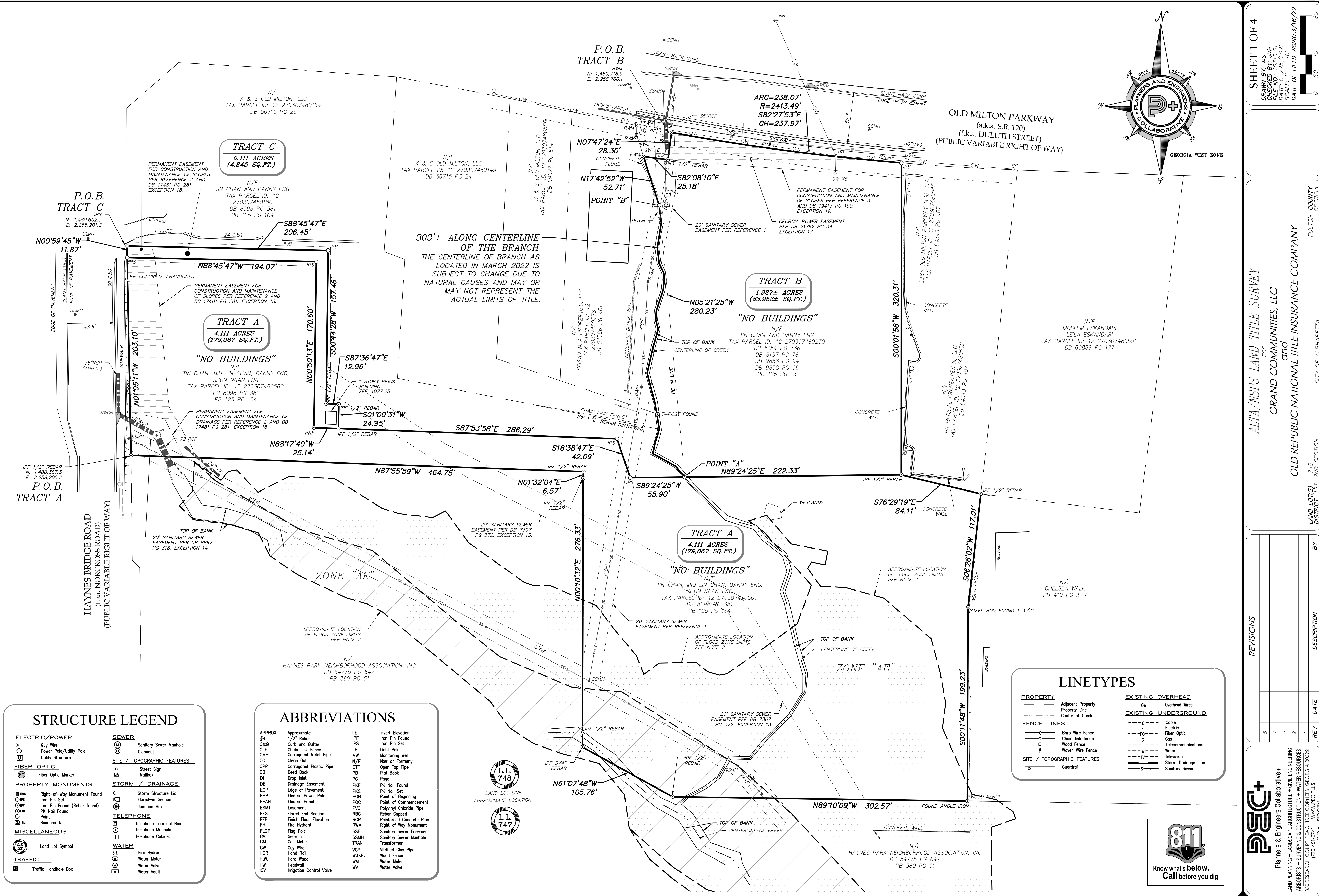


Z2

SHEET

U:\2024\15151501\15151501\Drawings\15151501 - ALTA.dwg - G:\Molloy - 6/28/2024 12:31 PM

This drawing is the property of Planform and Engineers Collaborative and is not to be copied, reproduced, or used in any way without the written consent of Planform and Engineers Collaborative. It is not to be used on any other project and is to be returned upon request. © Planform and Engineers Collaborative.



7/1/2022

Re: **Letter of Intent**
Old Milton Parkway (+/- 6.149 acres)
PEC+ Project No. 15315.01

Dear Community Development officials,

This rezoning application is being submitted on behalf of the developer and applicant. This application proposes to rezone the approximately 6-acre property located on the south side of Old Milton Parkway from R-12 and O-I to DT-LW. This rezoning would facilitate the development of a new 24-unit single-family attached townhome community to be named "The Post" and is inspired by the city's start as a trading post in 1858 before growing into the community that it has become.

Existing Conditions:

The uses surrounding the property include:

- North: Office uses
- East: Chelsea Walk townhomes
- South: Undeveloped land and Haynes Park townhomes
- West: Undeveloped land, retail and Montessori school

As it currently exists, the subject property is located on the south side of Old Milton Parkway. The tract is undeveloped with a 20-foot sanitary sewer easement running along the west and south edge of the property. There are also streams and a floodplain located on the site.

Proposed Development

The proposed development consists of 24 single-family attached units (townhomes) and the units will be located solely along the portion the subject property that abuts Old Milton Parkway. Due to the almost 1.5 acres of floodplain and the location of the stream buffers, the overall density will be 3.9 units per acres; noticeably under the maximum allowed density for townhomes. The location and density of this proposed development falls within the Mixed-Use Live Work Future Land Use designation and will support the nearby Central Business District without impacting the Low-Density Residential land uses farther west.

The proposed development will be accessed from Old Milton Parkway, about 700 feet east of where the parkway intersects Haynes Bridge Road; there will be no vehicular access to any of the neighboring properties. There will be pocket parks spaced throughout the development to provide greenspace access to future residents, along with a mail kiosk located at the most southernly end of the project. The proposed units along the east side of the property will be buffered from the neighboring office use by a 20-foot planted buffer and the units to the west shall be separated by at least 30-feet of greenery and stream buffers. There is a stormwater facility proposed near the south end of the developable portion of the site that would collect runoff during significant rain events and mitigate impacts to the stream.

As previously mentioned, the location of the floodplain and stream buffers has pushed the developable area onto about 2 acres of land. We would therefore like to request a stream buffer variance to allow the project to encroach into the streams undisturbed and impervious setback. The remaining 4 acres of the site will continue in an undisturbed state and the area within the stream buffers that is to be encroached upon shall be revegetated and improved upon to mitigate potential effects of the site. Due to the existing constraints of the site, the design and location of the proposed development is deemed the best fit without infringing upon and negatively impacting the environmental aspects of the subject property. Exhibits have been attached to this application to show the potential for revegetation and management within the buffers.

6/30/2022

The applicant and owner respectfully request that the City of Alpharetta City Council, Planning Commission and Planning Staff to approve and support the Applicant's rezoning request to allow for the rezoning of this property from R-12 and O-I to DT-LW. This would facilitate the development of a new, 24-unit single-family attached townhome community that would contribute to the advancement of the purpose and intent of the City of Alpharetta comprehensive plan, creating a live-work environment for future residents with lower commute times and quality housing. The developer and their representatives welcome the opportunity to meet with all interested parties and representatives.

Sincerely,

Planners and Engineers Collaborative, Inc.



Kenneth J. Wood, P.E., LEED AP

President

For the Firm

kjw/ht/sl

7/1/2022

Re: **Zoning Standards Analysis**
Old Milton Parkway Rezoning (+/-6.149 acres)
PEC+ Project No. 15315.01

Dear Community Development officials,

Please see below the responses to the Alpharetta Planning Commission Review Criteria:

The following standards and factors are found to be relevant to the exercise of the city's zoning powers and shall govern the review of all proposed amendments to the official zoning map:

A. How will this proposal be compatible with surrounding properties?

The proposed rezoning will permit a use that is suitable in context to the use and development of adjacent and nearby properties. The proposal is a new, new 24-unit single-family attached townhome community located on the south side of Old Milton Parkway about 700 feet east from where the parkway intersects Haynes Bridge Road. Given the site's location along a major thoroughfare (Old Milton Parkway) and its vicinity to office and retail uses, the proposed land use of medium density residential townhomes is reasonable at this location. The proposal also matches the land use of the townhome complex to the south and east, and acts as a supporting use to Alpharetta's City Center to the northwest. The proposal would have access only onto Old Milton Parkway, and as such the nearby properties who will not be affected by the proposal.

B. How will this proposal affect the use and value of the surrounding properties?

The zoning proposal will not adversely affect the existing use or usability of adjacent or nearby properties. Most of the nearby properties are already developed into residential, office or retail uses with portions of wooded land to separate them. The proposal includes measures to ensure compatibility to minimize effects on neighboring properties, primarily in leaving about 4 acres of the of the subject property in its current natural state and to remain outside the floodplain limits.

C. Can the property be developed for a reasonable economic use as currently zoned? Please explain why or why not.

The proposal loses much of its economic use because of factors that are outside of the applicant's control. More than half of the property is undevelopable due to the floodplain to the south and the extent of the stream buffers and setbacks. Under its current zoning designation, R-12 and O-I, the site is limited in its development potential. Rezoning the property to DT-LW will allow the site to be effectively and efficiently designed to provide a far more reasonable economic use without causing strain to the nearby infrastructure and facilities.

D. What would be the increase to population and traffic if the proposal were approved?

The proposed rezoning will not result in a use which will or could cause an excessive or burdensome use of existing streets or transportation facilities. The single-family attached units are targeted toward younger families, young professionals, and older persons looking to downsize. Additionally, a traffic generation report has been included in this submittal and anticipates a trip generation of 132 overall trips in and out of the site over a 24-hour period; far less than the majority of proposed residential developments.

E. What would be the impact to schools and utilities if the proposal were approved?

The proposed rezoning will not result in a use which will or could cause an excessive or burdensome use of existing utilities or schools. As previously mentioned, with the units geared towards young professionals and individuals looking to downsize, the student population should remain unaffected. Utilities on-site are being explored by the development team; the developer will make upgrades (if any) to facilitate the development. The site plan includes a stormwater management facility to collect runoff from significant rain events, so nearby properties will not experience flooding from this site.

F. How is the proposal consistent with the City of Alpharetta Comprehensive Plan, particularly the Future Land Use Map?

The proposed rezoning is in conformity with the policy and intent of the comprehensive plan. The Plan identifies the site as part of the 'Mixed-Use Live Work' land use area and is directly on the cusp of Central Business District designations and explicitly supports the proposed DT-LW zoning district. The proposed use would strengthen the workplace centers and nearby business and light industrial districts, which contribute to the overall economic development and managed that is encouraged and supported within the comprehensive plan.

G. Are there existing conditions which affect the development of the property and support the proposal request?

The site should be rezoned to facilitate the proposed development for several reasons, but perhaps the most compelling is the site's location. The area surrounding the site has become a major activity center in the City of Alpharetta and is only going to continue to grow as the city itself grows. This plan is a forward-thinking proposal that will provide additional high-quality housing in an area that will support a growing population and economic development.

Sincerely,
Planners and Engineers Collaborative, Inc.



Kenneth J. Wood, P.E., LEED AP
President

For the Firm

kjw/ht/sl

LEGAL DESCRIPTION
OVERALL TRACT

ALL THAT TRACT OR PARCEL OF LAND lying and being in the Land Lots 748 of the 1st District, 2nd Section, City of Alpharetta, Fulton County, Georgia and being more particularly described as follows:

BEGIN at the found right of way monument, said monument coordinates of North: 1,408,718.8 and East: 2,258,760.1, coordinates based on NAD83 State Plane Coordinate system, Georgia West zone, said monument located on the southerly right of way line of Old Milton Parkway (a.k.a. S.R. 120) (f.k.a. Duluth Street) (public variable right of way), said monument being the TRUE POINT OF BEGINNING;

THENCE along said southerly right of way of Old Milton Parkway along a curve turning to the left with an arc length of 238.07 feet, having a radius of 2413.49 feet, being subtended by a chord bearing of South 82 degrees 27 minutes 53 seconds East, and a chord length of 237.97 feet to a set 5/8 inch rebar with cap; thence leaving said southerly right of way of Old Milton Parkway and proceed South 00 degrees 01 minutes 58 seconds West a distance of 320.31 feet to a found 1/2 inch rebar; thence South 76 degrees 29 minutes 19 seconds East a distance of 84.11 feet to a found 1/2 inch rebar; thence South 06 degrees 26 minutes 02 seconds West a distance of 117.01 feet to a found 1 1/2 inch steel rod; thence South 00 degrees 11 minutes 48 seconds West a distance of 199.23 feet to a found angle iron located on the common land lot line between Land Lots 747 and 748; thence along said common land lot line North 89 degrees 10 minutes 09 seconds West a distance of 302.57 feet to a found 1/2 inch rebar; thence leaving said common land lot line and proceed North 61 degrees 07 minutes 48 seconds West a distance of 105.76 feet to a found 3/4 inch rebar; thence North 00 degrees 10 minutes 32 seconds East a distance of 276.33 feet to a found 1/2 inch rebar; thence North 01 degrees 32 minutes 04 seconds East a distance of 6.57 feet to a found 1/2 inch rebar; thence North 87 degrees 55 minutes 59 seconds West a distance of 464.75 feet to a found 1/2 inch rebar located on the easterly right of way of Haynes Bridge Road (f.k.a. Norcross Road) (public variable right of way); thence along said easterly right of way of Haynes Bridge Road the following courses and distances: North 01 degrees 05 minutes 11 seconds West a distance of 203.10 feet to a set 5/8 inch rebar with cap; North 00 degrees 59 minutes 45 seconds West a distance of 11.87 feet to a set 5/8 inch rebar with cap; thence leaving said easterly right of way and proceed South 88 degrees 45 minutes 47 seconds East a distance of 206.45 feet to a set 5/8 inch rebar with cap; thence South 00 degrees 44 minutes 28 seconds West a distance of 157.46 feet to a found 1/2 inch rebar; thence South 87 degrees 36 minutes 47 seconds East a distance of 12.96 feet to a found 1/2 inch rebar; thence South 01 degrees 00 minutes 31 seconds West a distance of 24.95 feet to a found 1/2 inch rebar; thence South 87 degrees 53 minutes 58 seconds East a distance of 286.29 feet to a set 5/8 inch rebar with cap; thence South 18 degrees 38 minutes 47 seconds East a distance of 42.09 feet to a set 5/8 inch rebar with cap; thence North 89 degrees 24 minutes 25 seconds East a distance of 55.90 feet more or less to a point at the centerline of the creek branch, said point being referred to as Point "A" (the commencement point of a tie-in line "A"- "B"); thence following the centerline of said Alcovy River and the meanderings thereof 303 feet more or less to a point, said point being referred to as point "B", (the terminus of said tie-in line "A"- "B"), said tie-in line from point "A" and to point "B" having the course of North 05 degrees 21 minutes 25 seconds West and a distance of 280.23 feet, more or less, to a point at the centerline of said creek branch; thence leaving the centerline of said creek branch and proceed North 17 degrees 42 minutes 52 seconds West a distance of 52.71 feet to a found right of way monument located on said southerly right of way of Old Milton Parkway; thence along said southerly right of way of Old Milton Parkway the following courses and distances: South 82 degrees 08 minutes 10 seconds East a distance of 25.18 feet to a found 1/2 inch rebar; North 07 degrees 47 minutes 24 seconds East a distance of 28.30 feet to a found right of way monument, said monument being the TRUE POINT OF BEGINNING.

Contains 267,865 square feet 6.149 acres, more or less.





LEFT SIDE / HIGH IMPACT ELEVATION



FRONT ELEVATION



COPYRIGHT ©2021 | FISCHER HOMES, INC. | ALL RIGHTS RESERVED.

THE TUSTIN | TUDOR ECLECTIC EXTERIOR

NOT FOR CONSTRUCTION



360
STUDIO



Planners & Engineers
Collaborative+

OLD MILTON PARKWAY

CITY OF ALPHARETTA, GA

TOWNHOME ELEVATIONS





LEFT SIDE / HIGH IMPACT ELEVATION



FRONT ELEVATION



COPYRIGHT ©2021 | FISCHER HOMES, INC. | ALL RIGHTS RESERVED.

THE BROOKLINE | TUDOR ECLECTIC EXTERIOR

NOT FOR CONSTRUCTION





Entry Monument Concept for *'The Post'*

06.27.2022

COPYRIGHT ©2022 | FISCHER HOMES, INC. | ALL RIGHTS RESERVED.

SPECIMEN TREE NOTE

SPECIMEN TREE REPORT COMPLETED ON 01/11/2018 BY ROOT ZONE TREE CONSULTANTS:
ALEX PHILLIPS, MA-4868A
ISA CERTIFIED ARBORIST®
ISA MEMBER
ISA TRAQ

SPECIMEN TREE SIZE

LARGE HARDWOODS 30 INCHES
LARGE SOFTWOODS 30 INCHES
FLOWERING UNDERSTORY 10 INCHES

*SURVEY ALL 18 INCH TREES

NOTES:

- OFFSITE TREES ARE NOT INCLUDED IN SITE DENSITY OR TREE PRESERVATION CALCULATIONS.
- TREE PROTECTION AND REPLACEMENT DETAILS AND NOTES ARE LOCATED ON SHEET TPR3.

SHRUB PLANTING SCHEDULE

SYMBOL	CODE	QUANTITY	BOTANICAL NAME	COMMON NAME	CONT.	MIN. HT.	SPACING
⊗	CAX	18	Callicarpa americana	American Beautyberry	1 gal	24"	As Shown
⊗	FOT	23	Fothergilla major 'Mount Airy'	Mount Airy Fothergilla	3 gal	24"	As Shown
▲	GSC	26	Gelsemium sempervirens	Jessamine Espalier	3 gal	24"	As Shown
⊗	HQX	7	Hydrangea quercifolia	Oakleaf Hydrangea	3 gal	24"	As Shown
⊗	IFX	42	Illicium floridanum	Purple Anise	3 gal	24"	As Shown
⊗	IAS	15	Ilex x attenuata 'Savannah'	Savannah Holly	1 gal	24"	As Shown
⊗	IGX	23	Ilex glabra	Inkberry Holly	3 gal	24"	As Shown
⊗	IOX	13	Ilex opaca	American Holly	1 gal	24"	As Shown
⊗	IPX	36	Illicium parviflorum	Anise Tree	1 gal	24"	As Shown
⊗	LHX	54	Ligustrum howardii	Yellow-tip Ligustrum	3 gal	24"	As Shown
⊗	LCR	37	Loropetalum chinense 'Ruby'	Ruby Loropetalum	3 gal	24"	As Shown
⊗	MCX	24	Myrica cerifera	Wax Myrtle	1 gal	24"	As Shown
⊗	OR	42	Osmunda regalis	Royal Fern	1 gal	24"	As Shown
⊗	RCX	15	Rhododendron canadense	Wild Azalea	1 gal	24"	As Shown
⊗	VAX	7	Vaccinium ashei	Rabbit Eye Blueberry	1 gal	24"	As Shown

GRASSES AND PERENNIALS

AV	347	Andropogon virginicus	Broomsedge Bluestem	1 gal	24" o.c.	As Shown
CL	241	Chasmanthium latifolium	Wood Oats	1 gal	24" o.c.	As Shown
EJ	106	Eupatorium fistulosum	Joe Pye Weed	1 gal	24" o.c.	As Shown
IV2	264	Iris virginica	Blue Flag Iris	1 gal	18" o.c.	As Shown
JE	633	Juncus effusus	Soft Rush	1 gal	18" o.c.	As Shown
NLX	708	Nuphar lutea	Yellow Pond-lily	1 gal	24" o.c.	As Shown
NMX	417	Nymphaea mexicana	Mexican Water Lily	1 gal	24" o.c.	As Shown
NO	267	Nymphaea odorata	Fragrant Water Lily	1 gal	24" o.c.	As Shown
PV	208	Panicum virgatum	Switch Grass	1 gal	30" o.c.	As Shown

PARKING CALCULATIONS:

106 PARKING SPACES

REQUIRED: 1 TREE PER 8 SPACES: 14 TREES
(106 / 8 = 13.25)

PROVIDED: *20 TREES
*PARKING LOT TREES ARE SHADED ON PLAN

REQUIRED: 1 PARKING LOT ISLAND PER 10 SPACES (106 / 10 = 10.6)
PROVIDED: 12 ISLANDS

REQUIRED: 10% MINIMUM: OF PARKING LOT AREA SHALL BE LANDSCAPED (52,125.75 SQFT X .1 = 5,212)
PROVIDED: 5,212 SQFT

PROVIDED: 6,966.31 (13.4%)

TREE PRESERVATION CALCULATIONS:

SITE AREA: 12.34 ACRES

AREA OF CREEK AND BUFFERS: -4.916 ACRES

ADJUSTED SITE AREA: 7.424 ACRES

TREE PRESERVATION:
REQUIRED TREE PRESERVATION:
120" DBH PER ACRE

7.424 X 120 = 890.88" DBH REQUIRED

EXISTING TREES SAVED ONSITE = *6,453.30" DBH

*SEE TREE SAMPLING DATA AND CALCULATIONS ON SHEET TPR.1

REMAINING DBH TO BE APPLIED TO SITE DENSITY AND SPECIMEN RECOMPENSE: 6,453.30 DBH -890.88 DBH 5,562.42 DBH

TREE DENSITY CALCULATIONS:

SITE AREA: 12.34 ACRES

AREA OF CREEK AND BUFFERS: -4.916 ACRES

ADJUSTED SITE AREA: 7.424 ACRES

SITE DENSITY CALCULATIONS:

REQUIRED TREE DENSITY = 30 UNITS PER ACRE

7.424 ACRE x 30 UNITS = 222.72 UNITS

SITE DENSITY UNITS REQUIRED = 222.72 UNITS

EXISTING TREE SAVE UNITS = *1,924.77 UNITS

* SEE TREE SAMPLING DATA AND CALCULATIONS ON SHEET TPR.1

SITE DENSITY IS MET WITH EXISTING TREE SAVE UNITS.

AVERAGE TREE SIZE IN SAMPLE AREAS: 13" DBH

11" DBH = 4 UNITS

222.72 / 4 = 55.68 TREES

55.68 X 13" DBH = 723.84 DBH

REMAINING DBH OF TREE SAVE AFTER MEETING PRESERVATION TO BE APPLIED TO SPECIMEN RECOMPENSE: 5,562.42 DBH -723.84 DBH 4,838.58 DBH

SPECIMEN RECOMPENSE CALCULATIONS:

SPECIMEN RECOMPENSE:

SPECIMEN TREES REMOVED (EXCLUDING DDH) TO BE REPLACED BY A FACTOR OF 1.5 TIMES:
449 DBH X 1.5 = 673.5 DBH

SPECIMEN RECOMPENSE REQUIRED = 674 DBH
SPECIMEN RECOMPENSE PROVIDED = *4,838.58 DBH

*DBH REMAINING AFTER FULFILLING TREE PRESERVATION AND SITE DENSITY REQUIREMENTS SATISFIES SPECIMEN RECOMPENSE.

LANDSCAPE & IRRIGATION

- IRRIGATION TO BE DESIGNED AND BUILT BY OTHERS.
- A R.O.W. MOWING AND MAINTENANCE AGREEMENT IS REQUIRED FOR THE APPLICANT TO MAINTAIN R.O.W PLANTINGS.
- SHOW LOCATION, TYPE, SIZE, AND DIRECTION OF SPRAY OF ANY IRRIGATION LINES AND HEADS PROPOSED ON THE R.O.W. MANUAL SHUT OFF VALVE TO BE BEHIND R.O.W. LINE. ALL IRRIGATION SYSTEMS ON THE R.O.W. MUST BE WRAPPED IN METALLIC TAPE DURING INSTALLATION.

TREE PLANTING SCHEDULE

SYMBOL	Code	Quantity	PERCENTAGE	OVERSTORY	EVERGREEN	BOTANICAL	COMMON	CONT.	CAL	MIN. HT.	UNITS	TOTAL UNITS	TOTAL INCHES
⌚	ARO	21	27.27%	Y		Acer rubrum 'October Glory'	October Glory Maple	B & B	2" CAL	12'-14'	0.4	8.4	42
⌚	IAF	3	3.90%		Y	Ilex x attenuata 'Foster No. 2'	Foster No. 2 Holly	B & B	N/A	10'-12'	0.4	1.2	N/A
⌚	JVB	3	3.90%		Y	Juniperus virginiana 'Brodie'	Brodie Columnar Cedar	B & B	N/A	8'-10'	0.4	1.2	N/A
⌚	LUM	9	11.69%			Lagerstroemia x 'Muskogee'	Lavender Crape Myrtle STANDARD	B & B	3" CAL	10'-12'	0.5	4.5	27
⌚	PCK	12	15.58%			Pistacia chinensis 'Keith Davey'	Keith Davey Chinese Pistache	B & B	3.5" CAL	12'-14'	0.5	6	42
⌚	PYS	9	11.69%			Prunus x yedoensis 'Shidare Yoshino'	Yoshino Cherry	B & B	2.5" CAL	10'-12'	0.4	3.6	22.5
⌚	QNX	12	15.58%	Y		Quercus nuttallii	Nuttall Oak	B & B	2.5" CAL	12'-14'	0.4	4.8	30
⌚	TDS	8	10.39%	Y		Taxodium distichum 'JFS-SGPN' STANDARD	Green Wisper Bald Cypress	B & B	3.5" CAL	12'-14'	0.5	4	28
TOTALS:		77	100.00%	53.25%	7.79%							33.7	191.5

POND TREE PLANTING SCHEDULE

⌚	BND	3		Y		Betula nigra 'Duraheat'	Duraheat River Birch Std.	B & B	2" CAL	12'-14'	N/A	N/A	N/A
⌚	CFX	11				Cornus florida	Eastern Dogwood	B & B	2" CAL	10'-12'	N/A	N/A	N/A

24 HOUR CONTACT:

SCALE 1" = 30'-0"

GEORGIA811
www.Georgia811.com
Know what's below.
Call before you dig.



360
STUDIO

THE LANDSCAPE ARCHITECTURE STUDIO OF
PLANNERS & ENGINEERS COLLABORATIVE

350 RESEARCH COURT
PEACHTREE CORNER,
GEORGIA 30092

O: 770.451.2741
PEC360STUDIO.COM

THIS DOCUMENT, ELECTRONIC AND
REPRODUCTIONS, IS THE EXCLUSIVE PROPERTY
OF 360 STUDIO AND IS NOT TO BE REPRODUCED OR
COPIED WHOLE OR IN PART EXCEPT AS
REQUIRED FOR THE PROJECT HEREIN. IT MAY
NOT BE USED ON ANY OTHER PROJECT WITHOUT
AN EXPRESSED WRITTEN AGREEMENT WITH 360
STUDIO.

PROJECT

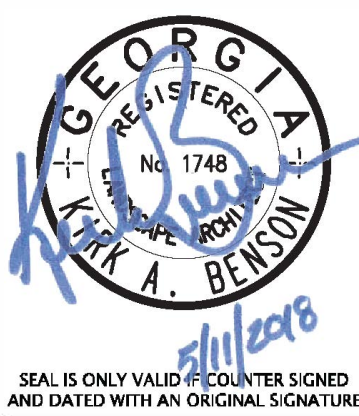
OLD MILTON
PARKWAY (THE
POST) STREAM
BUFFER
MITIGATION
EXAMPLE

REVISION DATE

DRAWN BY:
APPROVED BY:

PROJECT NUMBER

SEAL



SEAL IS ONLY VALID IF COUNTER SIGNED
AND DATED WITH AN ORIGINAL SIGNATURE

DATE

05/11/2018

TITLE

STREAM BUFFER
MITIGATION PLAN
EXAMPLE

SHEET

SPECIMEN TREE REPORT

City of Alpharetta

Surveyed by: James Mahoney ISA#: SO:10291A

Project # 15315.01

TREE REPORT FOR:

GRAND COMMUNITIES, LLC 3940 OLYMPIC BLVD SUITE 400 ERLANGER, KY 41018

PROPERTY ADDRESS:

OLD MILTON PKWY (2325) @ NORCROSS ST (0 & 210) @ HAYNES BRIDGE RD (11775) LAND LOT# 748. 12TH DISTRICT, CITY OF ALPHARETTA, GEORGIA

Specimen Tree Inventory

Some trees on a site warrant special consideration and encouragement for preservation. Specifications for these trees are established under the City of Alpharetta's Tree Preservation and Replacement Regulations. The intent of these specifications is to provide the necessary information to facilitate project design, plan review and enforcement processes. The purpose is to make the city of Alpharetta a more attractive place to live, provide a healthy living environment, and better control of storm water runoff, noise, glare and soil erosion.

The City of Alpharetta Specimen tree specifications are organized by size:

SWEETGUM AND POPLAR TREES 30" DBH

PINE TREES 30" DBH

ALL OTHER TREES 24" DBH

CONIFEROUS TREES 20" DBH

BEECH, TUPELO, PERSIMMON, SASSAFRAS, MAGNOLIA 20" DBH

FLOWERING UNDERSTORY TREES 8" DBH

SOURWOOD TREES 10" DBH

And condition:

- Life expectancy greater than 15 years

- Relatively sound and solid trunk with no visible decay

- No more than one major and several minor dead limbs (hardwoods)

- No major insect or pathological problems

Site Location

The site is located in the city of Alpharetta, it South of Old Milton Parkway and East of Haynes Bridge Road. It is directly adjacent to “My First Academy”, a children’s Montessori School, that the site partials surrounds. The site is also bordered to the north west by a small shopping plaza, and Townhomes along its eastern border. The southern edge of the property is adjacent to another townhome development, but is buffered by a small existing forest and a walking trail. The site is covered by existing woodlands, it is predominantly poplars, with a good number of water oaks spread throughout. There are a concentration of pines on the southwestern portion of the site. The property is bisected by multiple streams and has a considerable area of floodplain along its southern extent. Overall the site appears to be healthy.

Definitions

Tree Number: Trees are tagged with an aluminum disk that shows a unique number to identify the tree.

Species: Trees are listed by a regional common name and botanical name.

Diameter at Breast Height (DBH): The diameter of a trunk at 4.5’ above ground level. If tree is split, measurement is taken at narrowest point below bifurcation. Measured in inches.

Condition:

Excellent: A specimen tree that is a State Champion and warrants saving at all costs. This classification would be confirmed by the County Arborist and the Georgia Forestry Council.

Good: A specimen tree with healthy productive tip growth. A sound trunk with no visible damage or decay. No major limb loss and healthy branch unions. No visible insect or disease infestations. Life expectancy of more than 15 years.

Fair: A specimen tree with healthy but not vigorous tip growth. Less than 30% of crown is dead. No major dead limbs and no major trunk cavities or damage. Branch unions show some signs of stress. Tree is expected to live longer than 10 years.

Poor: More than 30% of the crown is dead or has significant tip die back. More than one major limb is dead and are large trunk cavities with visible decay. Severe insect or disease damage leading to immediate death. Roots are visible and show signs of decay and rot. Life expectancy is less than 10 years.

DDH: Tree has no bud or leaf production. All limbs are barren and rot is visible, or there is severe or uncorrectable damage that will lead to a loss of property or life if there is tree failure.

Invasive: Tree species whose native range is not within the Piedmont classification.

Specimen Tree Summary: Most of the specimen sized trees on site Meet the city of Alpharetta specimen standards for specimen trees.

Total Specimen Sized and Quality Trees: 27

Excellent Condition 0

Good Condition: 21

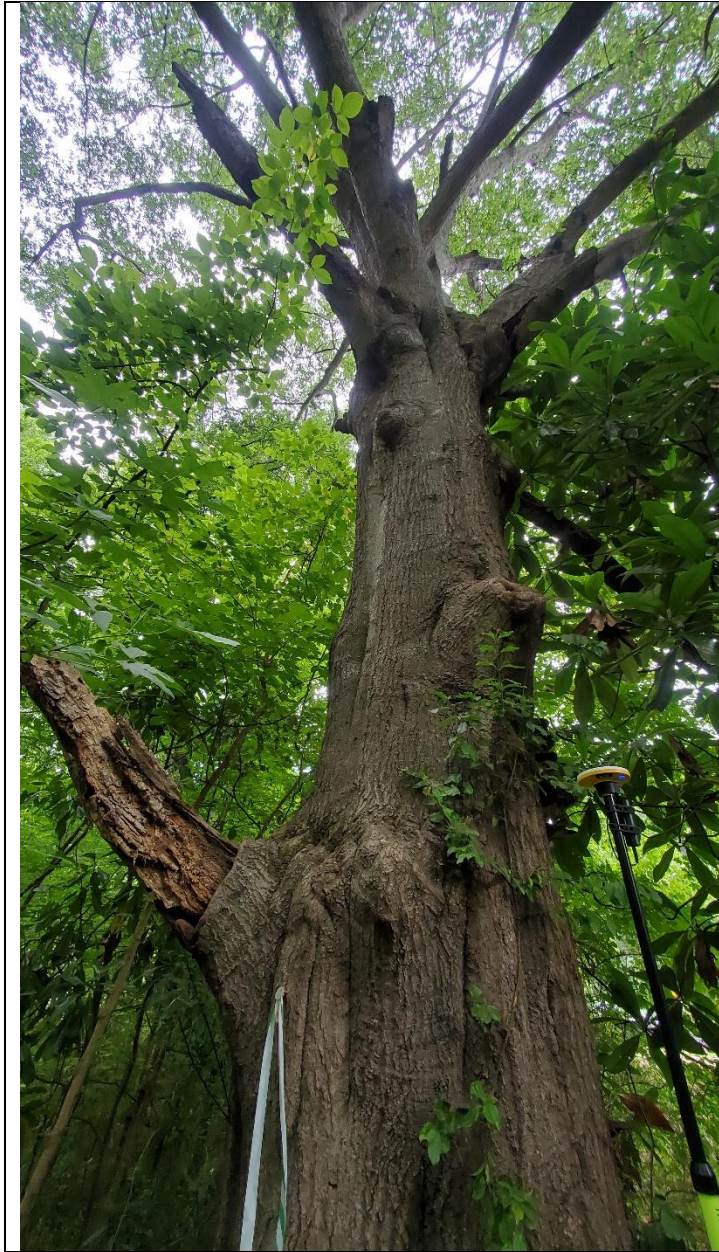
Fair Condition: 3

Poor Conditions: 3

SPECIMEN TREE AND QUALITY TREE DATA					
Tree #	DBH "	Common name	Scientific name	Condition	Status
76	32	WATER OAK	<i>Quercus nigra</i>	FAIR	Tree #76 is a Water Oak, it has a DBH of 32 inches when measured at 4.5' from the ground and has been tagged with an aluminum tag showing the Tree number. Tree #76 is a Tree of Quality.
304	48	WATER OAK	<i>Quercus nigra</i>	POOR	Tree #304 is a Water Oak, it has a DBH of 48 inches when measured at 4.5' from the ground and has been tagged with an aluminum tag showing the Tree number. Tree #304 is a DDH. The tree meets this designation due to it having a major Trunk Wound and it having Fruiting Bodies. In addition the tree has 3 Broken Major Branches and 3 Broken Minor Branches.
305	28	WATER OAK	<i>Quercus nigra</i>	GOOD	Tree #305 is a Water Oak, it has a DBH of 28 inches when measured at 4.5' from the ground and has been tagged with an aluminum tag showing the Tree number. Tree #305 is a Tree of Quality.
308	30	SWEETGUM	<i>Liquidambar styraciflua</i>	GOOD	Tree #308 is a Sweetgum, it has a DBH of 30 inches when measured at 4.5' from the ground and has been tagged with an aluminum tag showing the Tree number. Tree #308 is a Tree of Quality.
311	38	PINE	<i>Pinus spp.</i>	GOOD	Tree #311 is a Pine, it has a DBH of 38 inches when measured at 4.5' from the ground and has been tagged with an aluminum tag showing the Tree number. Tree #311 is a Tree of Quality.
312	45	POPLAR	<i>Liriodendron tulipifera</i>	GOOD	Tree #312 is a Poplar, it has a DBH of 45 inches when measured at 4.5' from the ground and has been tagged with an aluminum tag showing the Tree number. Tree #312 is a Tree of Quality.
313	31	SWEETGUM	<i>Liquidambar styraciflua</i>	GOOD	Tree #313 is a Sweetgum, it has a DBH of 31 inches when measured at 4.5' from the ground and has been tagged with an aluminum tag showing the Tree number. Tree #313 is a Tree of Quality.
315	39	SWEETGUM	<i>Liquidambar styraciflua</i>	GOOD	Tree #315 is a Sweetgum, it has a DBH of 39 inches when measured at 4.5' from the ground and has been tagged with an aluminum tag showing the Tree number. Tree #315 is a Tree of Quality.
317	27	WATER OAK	<i>Quercus nigra</i>	GOOD	Tree #317 is a Water Oak, it has a DBH of 27 inches when measured at 4.5' from the ground and has been tagged with an aluminum tag showing the Tree number. Tree #317 is a Tree of Quality.
318	56	WATER OAK	<i>Quercus nigra</i>	GOOD	Tree #318 is a Water Oak, it has a DBH of 56 inches when measured at 4.5' from the ground and has been tagged with an aluminum tag showing the Tree number. Tree #318 is a Tree of Quality.
319	33	WATER OAK	<i>Quercus nigra</i>	GOOD	Tree #319 is a Water Oak, it has a DBH of 33 inches when measured at 4.5' from the ground and has been tagged with an aluminum tag showing the Tree number. Tree #319 is a Tree of Quality.

321	32	POPLAR	<i>Liriodendron tulipifera</i>	GOOD	Tree #321 is a Poplar, it has a DBH of 32 inches when measured at 4.5' from the ground and has been tagged with an aluminum tag showing the Tree number. Tree #321 is a Tree of Quality.
322	32	POPLAR	<i>Liriodendron tulipifera</i>	GOOD	Tree #322 is a Poplar, it has a DBH of 32 inches when measured at 4.5' from the ground and has been tagged with an aluminum tag showing the Tree number. Tree #322 is a Tree of Quality.
323	8	MAGNOLIA	<i>Magnolia grandiflora</i>	GOOD	Tree #323 is a Magnolia, it has a DBH of 8 inches when measured at 4.5' from the ground and has been tagged with an aluminum tag showing the Tree number. Tree #323 is a Tree of Quality.
324	39	WATER OAK	<i>Quercus nigra</i>	POOR	Tree #324 is a Water Oak, it has a DBH of 39 inches when measured at 4.5' from the ground and has been tagged with an aluminum tag showing the Tree number. Tree #324 is a DDH. The tree meets this designation due to it having Tip Dieback and it having a Split with Included Bark. In addition the tree has 9 Broken Minor Branches.
325	28	ELM	<i>Ulmus spp.</i>	GOOD	Tree #325 is a Elm, it has a DBH of 28 inches when measured at 4.5' from the ground and has been tagged with an aluminum tag showing the Tree number. Tree #325 is a Tree of Quality. it having a Split with Included Bark.
326	51	WATER OAK	<i>Quercus nigra</i>	POOR	Tree #326 is a Water Oak, it has a DBH of 51 inches when measured at 4.5' from the ground and has been tagged with an aluminum tag showing the Tree number. Tree #326 is a DDH. The tree meets this designation due to it having a major Trunk Wound and it having Fruiting Bodies as well as it having a Split with Included Bark.
1387	28	POPLAR	<i>Liriodendron tulipifera</i>	GOOD	Tree #1387 is a Poplar, it has a DBH of 28 inches when measured at 4.5' from the ground and has been tagged with an aluminum tag showing the Tree number. Tree #1387 is a Tree of Quality.
1388	27	WATER OAK	<i>Quercus nigra</i>	GOOD	Tree #1388 is a Water Oak, it has a DBH of 27 inches when measured at 4.5' from the ground and has been tagged with an aluminum tag showing the Tree number. Tree #1388 is a Tree of Quality.
1389	30	POPLAR	<i>Liriodendron tulipifera</i>	GOOD	Tree #1389 is a Poplar, it has a DBH of 30 inches when measured at 4.5' from the ground and has been tagged with an aluminum tag showing the Tree number. Tree #1389 is a Tree of Quality.
1399	24	RED MAPLE	<i>Acer rubrum</i>	GOOD	Tree #1399 is a Red Maple, it has a DBH of 24 inches when measured at 4.5' from the ground and has been tagged with an aluminum tag showing the Tree number. Tree #1399 is a Tree of Quality.

1400	25	RED MAPLE	<i>Acer rubrum</i>	GOOD	Tree #1400 is a Red Maple, it has a DBH of 25 inches when measured at 4.5' from the ground and has been tagged with an aluminum tag showing the Tree number. Tree #1400 is a Tree of Quality.
1401	16	BOX ELDER	<i>Acer negundo</i>	GOOD	Tree #1401 is a Box Elder, it has a DBH of 16 inches when measured at 4.5' from the ground and has been tagged with an aluminum tag showing the Tree number. Tree #1401 is a Tree of Quality.
1402	32	POPLAR	<i>Liriodendron tulipifera</i>	GOOD	Tree #1402 is a Poplar, it has a DBH of 32 inches when measured at 4.5' from the ground and has been tagged with an aluminum tag showing the Tree number. Tree #1402 is a Tree of Quality.
1403	24	WATER OAK	<i>Quercus nigra</i>	GOOD	Tree #1403 is a Water Oak, it has a DBH of 24 inches when measured at 4.5' from the ground and has been tagged with an aluminum tag showing the Tree number. Tree #1403 is a Tree of Quality.
1404	9	DOGWOOD	<i>Cornus spp.</i>	FAIR	Tree #1404 is a Dogwood, it has a DBH of 9 inches when measured at 4.5' from the ground and has been tagged with an aluminum tag showing the Tree number. Tree #1404 is a Tree of Quality.
1405	9	DOGWOOD	<i>Cornus spp.</i>	FAIR	Tree #1405 is a Dogwood, it has a DBH of 9 inches when measured at 4.5' from the ground and has been tagged with an aluminum tag showing the Tree number. Tree #1405 is a Tree of Quality.
Total	821				



Tree #304 is a Water Oak, it has a DBH of 48 inches when measured at 4.5' from the ground and has been tagged with an aluminum tag showing the Tree number. Tree #304 is a DDH. The tree meets this designation due to it having a major Trunk Wound and it having Fruiting Bodies. In addition the tree has 3 Broken Major Branches and 3 Broken Minor Branches. Further consideration should be granted to this tree due to its close proximity to an active road to which it poses a large risk.



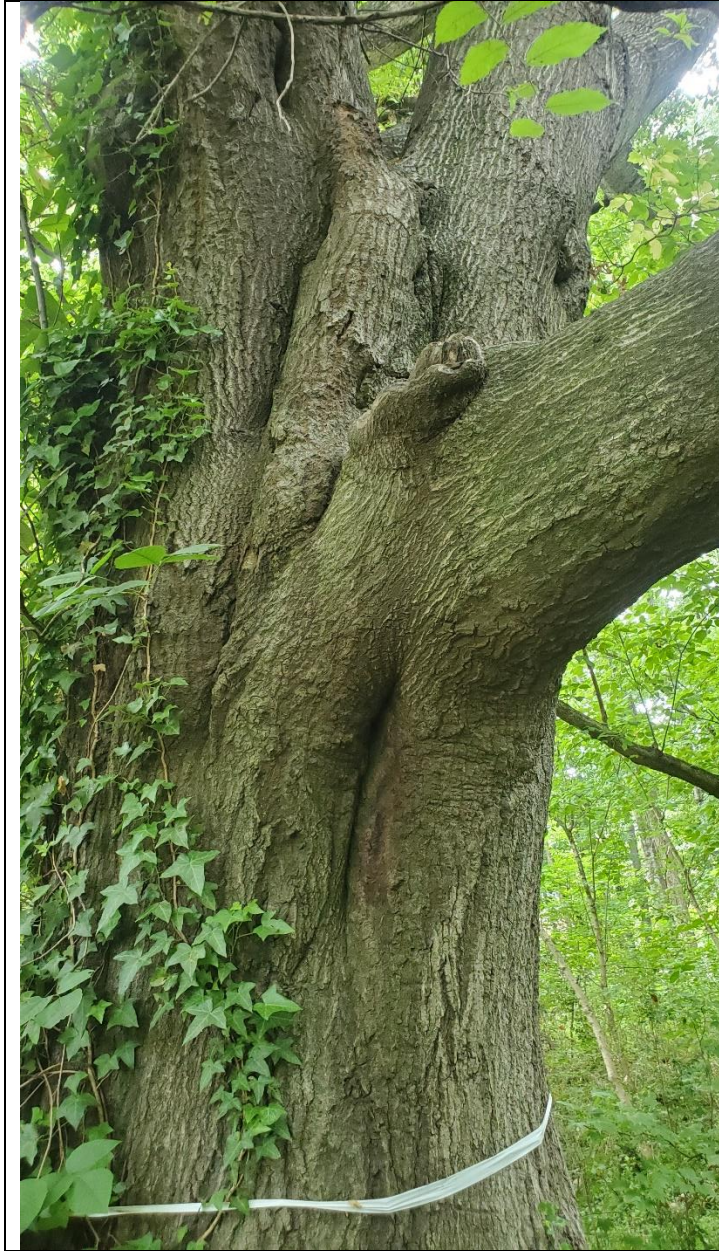
Tree #304 is a Water Oak, it has a DBH of 48 inches when measured at 4.5' from the ground and has been tagged with an aluminum tag showing the Tree number. Tree #304 is a DDH. The tree meets this designation due to it having a major Trunk Wound and it having Fruiting Bodies. In addition the tree has 3 Broken Major Branches and 3 Broken Minor Branches. Further consideration should be granted to this tree due to its close proximity to an active road to which it poses a large risk.



Tree #324 is a Water Oak, it has a DBH of 39 inches when measured at 4.5' from the ground and has been tagged with an aluminum tag showing the Tree number. Tree #324 is a DDH. The tree meets this designation due to it having Tip Dieback and it having a Split with Included Bark. In addition the tree has 9 Broken Minor Branches. Further consideration should be granted to this tree due to its close proximity to an elementary school building and playground to which it poses a high risk.



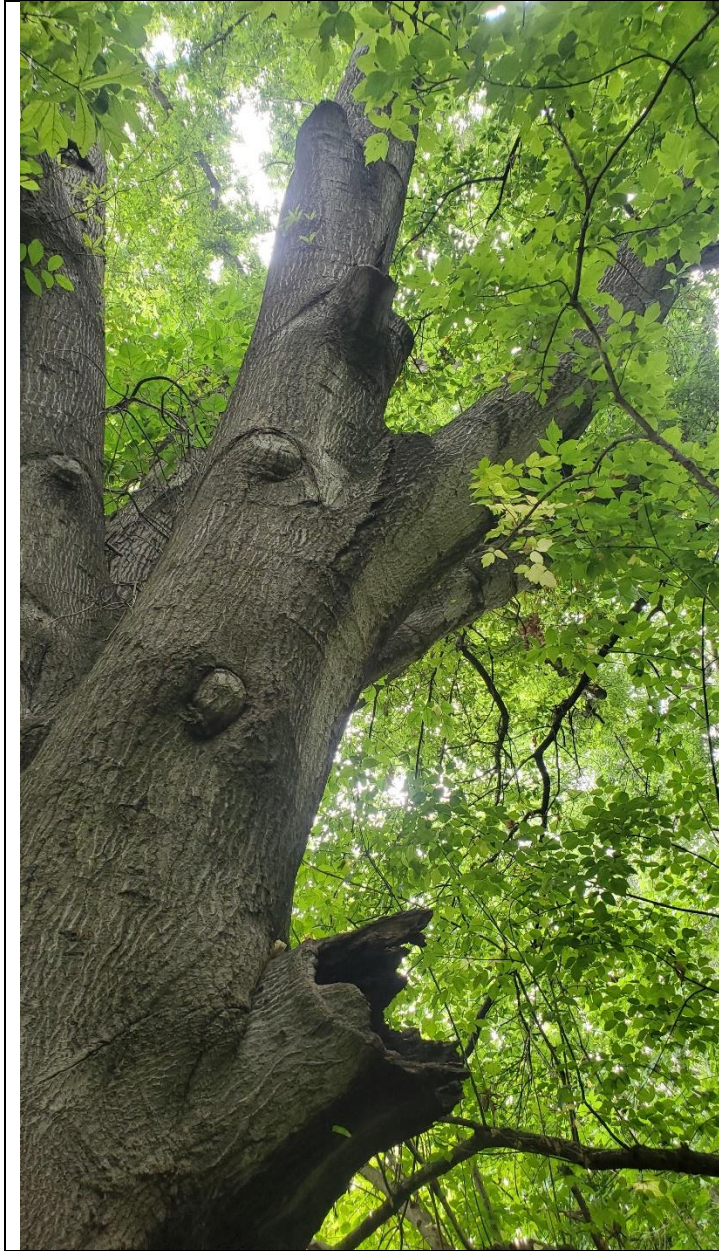
Tree #326 is a Water Oak, it has a DBH of 51 inches when measured at 4.5' from the ground and has been tagged with an aluminum tag showing the Tree number. Tree #326 is a DDH. The tree meets this designation due to it having a major Trunk Wound and it having Fruiting Bodies as well as it having a Split with Included Bark. Further consideration should be granted to this tree due to its close proximity to an active road to which it poses a large risk.



Tree #326 is a Water Oak, it has a DBH of 51 inches when measured at 4.5' from the ground and has been tagged with an aluminum tag showing the Tree number. Tree #326 is a DDH. The tree meets this designation due to it having a major Trunk Wound and it having Fruiting Bodies as well as it having a Split with Included Bark. Further consideration should be granted to this tree due to its close proximity to an active road to which it poses a large risk.



Tree #326 is a Water Oak, it has a DBH of 51 inches when measured at 4.5' from the ground and has been tagged with an aluminum tag showing the Tree number. Tree #326 is a DDH. The tree meets this designation due to it having a major Trunk Wound and it having Fruiting Bodies as well as it having a Split with Included Bark. Further consideration should be granted to this tree due to its close proximity to an active road to which it poses a large risk.



Tree #326 is a Water Oak, it has a DBH of 51 inches when measured at 4.5' from the ground and has been tagged with an aluminum tag showing the Tree number. Tree #326 is a DDH. The tree meets this designation due to it having a major Trunk Wound and it having Fruiting Bodies as well as it having a Split with Included Bark. Further consideration should be granted to this tree due to its close proximity to an active road to which it poses a large risk.

TREE #	DBH "	SPECIES
76	32	WATER OAK
304	48	WATER OAK
305	28	WATER OAK
308	30	SWEETGUM
309	34	SWEETGUM
310	35	PINE
311	38	PINE
312	45	POPLAR
313	31	SWEETGUM
315	39	SWEETGUM
317	27	WATER OAK
318	56	WATER OAK
319	33	WATER OAK
321	32	POPLAR
322	32	POPLAR
323	8	MAGNOLIA
324	39	WATER OAK
325	28	ELM
326	51	WATER OAK
387	28	POPLAR
1388	27	WATER OAK
1389	30	POPLAR
1390	15	WILLOW OAK
1391	10	RED MAPLE
1392	3	ELM
1393	5	POPLAR
1394	9	BOX ELDER
1395	6	BOX ELDER
1396	16	SWEETGUM
1397	9	BOX ELDER
1398	30	SWEETGUM
1399	24	RED MAPLE
1400	25	RED MAPLE
1401	16	BOX ELDER
1402	32	POPLAR
1403	24	WATER OAK
1404	9	DOGWOOD
1405	9	DOGWOOD
1406	8	ASH
1407	19	BOX ELDER
1408	8	WALNUT
1409	16	ASH



SWEETGUM AND POPLAR TREES	30 INCHES
PINE TREES	30 INCHES
ALL OTHER TREES	24 INCHES
CONIFEROUS TREES	20 INCHES
BEECH, TUPELO, PERSIMMON, SASSAFRAS MAGNOLIA	20 INCHES
FLOWERING UNDERSTORY TREES	8 INCHES
SOURWOOD TREES	10 INCHES

SPECIMEN TREE REPORT COMPLETED 6-29-2022 BY ROOT ZONE TREE
CONSULTANTS:
JAMES MAHONEY
ISA CERTIFIED ARBORIST SO #10291A



OLD MILTON PKWY

FOR
GRAND COMMUNITIES, LLC
3940 OLYMPIC BLVD
SUITE 400
ERLANGER, KY 41018

OLD MILTON PKWY (2325) @ NORCROSS ST (0 & 210) @ HAYNES BRIDGER RD
(11775) LAND LOT# 748, 12TH DISTRICT, CITY OF ALPHARETTA, GEORGIA

ROOT ZONE TREE CONSULTANTS

350 RESEARCH COURT PEACHTREE CORNERS, GEORGIA 30092 (678) 684-6202 WWW.RZCONSULTANTS.COM

A DIVISION OF PLANNERS AND ENGINEERS COLLABORATIVE WWW.PECATL.COM

REVISIONS:

[illegible]

SPECIMEN TREE SURVEY

DATE: 6-29-2022
PROJECT: 15315.01

PRELIMINARY

NOT TO BE RELEASED FOR CONSTRUCTION



SHEET #

S1

OF

This drawing is the property of Planners and Engineers Collaborative and is not to be copied in whole or in part. It is not to be used on any other project and is to be returned upon request. Planners and Engineers Collaborative. ©

Filters

Code Enforcement

Filters

Styling

Filter as map moves ⓘ



Location

2325 OLD MILTON PARKWAY

No results

Select attribute filters (8)

☐ Type Description
3 values☐ Number
92 values☐ Tag
61 values☐ Status Code
1 values☐ Assigned To
2 values☐ Initiated Date
3/30/2017 to 8/10/2021

Showing 25 of 159 rows

[Close Table](#)

Type Description	Number	Tag	Status Code	Assigned To	Initiated Date	Location	Reference ID
Code Enforcement-Compl...	CE170033	Accessory Structures	OPEN		3/30/2017, 3:01 PM	12720 Bethany Road	11175
Code Enforcement-Trees	CE190025	Stop Work Order - Trees	OPEN		2/25/2019, 4:12 PM	1825 Mayfield Road	27978
Code Enforcement-Compl...	CE190036	Business vehicle in residential area	OPEN		3/11/2019, 2:51 PM	11170 Wittenridge Drive	28338
Code Enforcement-Compl...	CE190043	Business vehicles in residential a...	OPEN		4/2/2019, 3:02 PM	10585 Kingsmark Trail	28899
Code Enforcement-Compl...	CE190053	Tree removal without permit	OPEN		4/17/2019, 3:44 PM	5365 Derby Chase Court	29270
Code Enforcement-Compl...	CE190099	Structual Issues	OPEN		9/5/2019, 3:35 PM	44 Birch Rill Drive	32366
Code Enforcement-Compl...	CE190100	Drainage Violation	OPEN		9/5/2019, 4:01 PM	160 North Main Street	32367
Code Enforcement-Compl...	CE190107	Stop Work Order	OPEN		9/27/2019, 1:01 PM	10580 Tuxford Drive	32800
Code Enforcement-Compl...	CE190108	Stop Work Order	OPEN		9/27/2019, 1:09 PM	1230 Tuscany Court	32801
Code Enforcement-Compl...	CE200004	Stop Work Order	OPEN		1/14/2020, 3:44 PM	1565 Highview Pines Pass	34799
Code Enforcement-Compl...	CE200011	Stop Work Order	OPEN		2/7/2020, 11:38 AM	710 Tate Drive	35283
Code Enforcement-Compl...	CE200065	Deck in a State of Disrepair	OPEN	BESMITH	4/7/2020, 2:03 PM	1430 Hillcrest Heights	36677
Code Enforcement-Compl...	CE200074	R/W trashcan overflowing	OPEN		4/9/2020, 3:09 PM	762 North Main Street	36739
Code Enforcement-Compl...	CE200084	Complaint	OPEN	BSCHROEDER	5/6/2020, 3:55 PM	194 Mayfield Circle	37241
Code Enforcement-Compl...	CE200097	STOP WORK ORDER, High Grass...	OPEN		5/27/2020, 3:18 PM	1031 Colony Drive	37632
Code Enforcement-Trees	CE200110	Stop work order	OPEN		6/4/2020, 12:13 PM	4650 Lakeway Place	37806
Code Enforcement-Compl...	CE200130	Stop Work Order	OPEN		6/29/2020, 7:57 AM	645 Brook Landing Court	38319
Code Enforcement-Compl...	CE200131	Stop Work Order	OPEN		6/29/2020, 8:56 AM	11595 Vista Forest Drive	38324
Code Enforcement-Trees	CE200158	Undisturbed Buffer Violation	OPEN		7/27/2020, 1:21 PM	6331 Maid Marion Close	38920
Code Enforcement-Trees	CE200206	TREE REMOVAL WITHOUT PERMIT	OPEN		8/17/2020, 1:46 PM	315 Wood Trace Drive	39479
Code Enforcement-Compl...	CE200222	STOP WORK ORDER, Rear Deck	OPEN		8/26/2020, 3:03 PM	12255 Greenmont Walk	39699
Code Enforcement-Compl...	CE200225	Stop work order	OPEN		8/31/2020, 8:28 PM	5020 Southlake Drive	39808
Code Enforcement-Compl...	CE200232	Stop work order	OPEN		9/9/2020, 8:33 PM	2240 Lake Shore Landing	40027

ED 12/23/21

CONTINGENT SALE AGREEMENT

THIS CONTINGENT SALE AGREEMENT ("Agreement") is made on the Effective Date (defined below in Section 14) by and between GRAND COMMUNITIES, LLC, a Kentucky limited liability company ("Buyer") and TIN CHAN and MIU LIN CHAN, a married couple residing in Georgia, and DANNY ENG and SHUN NGAN ENG, a married couple residing in Georgia ("Seller") (collectively "Parties"). For good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged by the Parties, the Parties agree as follows:

1. **PURCHASE.** For the Purchase Price (defined below in Section 4), Seller shall sell to Buyer and Buyer shall purchase from Seller subject to the terms and conditions of this Agreement the following Real Estate (defined below in this Section 1):

a. **Real Estate.** Approximately 6.16 +/- acres, being PID 12-270307480560, 12-270307480230, and 12-270307480180, 2325 Old Milton Parkway, Alpharetta, Fulton County, Georgia, 11775 Haynes Bridge Road, Alpharetta, Fulton County, Georgia, and 0 Norcross Street, Alpharetta, Fulton County, Georgia and being the same property conveyed to Seller by Deed dated _____ and recorded _____ in Book _____, Page _____ in the Fulton County Recorder's Office ("Real Estate"). The Real Estate includes all rights, title and interests to: rights, ways, privileges, easements, escrows, structures, fixtures, systems, improvements, topsoil, trees, timber, landscaping, crops, plants, minerals (including oil and gas), entitlements, development rights, strips, gores, streets, alleys, ways adjoining or crossing the Real Estate, taps and other rights arising from, appertaining to or benefiting the Real Estate. The Real Estate is outlined on the Aerial Map attached hereto as Exhibit A. The Real Estate Legal Description is attached hereto as Exhibit B.

2. **REZONING PERIOD.** Buyer's obligation to close under this Agreement is contingent upon rezoning of the Real Estate to permit construction of single-family residential units as set out below. If Buyer is not completely satisfied with the Real Estate to its sole satisfaction at any such time during the Rezoning Period, Buyer may terminate this Agreement for any and all reason(s) by delivering notice to Seller on or before the expiration of the Rezoning Period, and the Deposit (defined below in Section 3) shall be handled per Section 3 of this Agreement. Buyer will use its best efforts its best efforts to timely, actively and diligently pursue rezoning of the Real Estate. Seller shall fully cooperate with Buyer in doing so. Buyer may elect to extend the Rezoning Period by making said election and providing written notice to Seller of same prior to the expiration of the then current period as described herein:

- a. **Rezoning Period.** The Rezoning Period shall commence upon the Effective Date and shall expire at midnight on May 30, 2022 ("Rezoning Period").
- b. **Rezoning Period Extension No. 1.** Rezoning Period Extension No. 1 shall commence upon the expiration date of the Rezoning Period and shall expire at midnight on July 4, 2022 ("Rezoning Period Extension No. 1").
- c. **Rezoning Period Extension No. 2.** Rezoning Period Extension No. 2 shall commence upon the expiration date of the Rezoning Period Extension No. 1 and shall expire at midnight on August 29, 2022 ("Rezoning Period Extension No. 2").

3. **EARNEST MONEY DEPOSIT.** Buyer has deposited \$ _____ ("Review Deposit") in escrow per the escrow agreement attached hereto as Exhibit C ("LOI Escrow Agreement"). By 5 business days from the Effective Date and upon execution of the escrow agreement attached hereto as Exhibit D ("Escrow Agreement"), the LOI Escrow Agreement shall terminate, Escrow Agent shall close the escrow account established pursuant to the LOI Escrow Agreement, shall transfer such Review Deposit into the escrow account as established by the Escrow Agreement, and Buyer shall deliver to the Escrow Agent to be held in escrow per the Escrow Agreement an additional earnest money

NO. 1 and Rezoning Period Extension NO. 2 Collectively referred to herein as "Rezoning Period."

CONTINGENT SALE AGREEMENT

THIS CONTINGENT SALE AGREEMENT ("Agreement") is made on the Effective Date (defined below in Section 14) by and between **GRAND COMMUNITIES, LLC**, a Kentucky limited liability company ("Buyer") and **TIN CHAN and MIU LIN CHAN**, a married couple residing in Georgia, and **DANNY ENG and SHUN NGAN ENG**, a married couple residing in Georgia ("Seller") (collectively "Parties"). For good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged by the Parties, the Parties agree as follows:

1. **PURCHASE.** For the Purchase Price (defined below in Section 4), Seller shall sell to Buyer and Buyer shall purchase from Seller subject to the terms and conditions of this Agreement the following Real Estate (defined below in this Section 1):
 - a. **Real Estate.** Approximately 6.16 +/- acres, being PID 12-270307480560, 12-270307480230, and 12-270307480180, 2325 Old Milton Parkway, Alpharetta, Fulton County, Georgia, 11775 Haynes Bridge Road, Alpharetta, Fulton County, Georgia, and 0 Norcross Street, Alpharetta, Fulton County, Georgia and being the same property conveyed to Seller by Deed dated _____ and recorded _____ in Book _____, Page _____ in the Fulton County Recorder's Office ("Real Estate"). The Real Estate includes all rights, title and interests to: rights, ways, privileges, easements, escrows, structures, fixtures, systems, improvements, topsoil, trees, timber, landscaping, crops, plants, minerals (including oil and gas), entitlements, development rights, strips, gores, streets, alleys, ways adjoining or crossing the Real Estate, taps and other rights arising from, appertaining to or benefiting the Real Estate. The Real Estate is outlined on the Aerial Map attached hereto as **Exhibit A**. The Real Estate Legal Description is attached hereto as **Exhibit B**.
2. **REZONING PERIOD.** Buyer's obligation to close under this Agreement is contingent upon rezoning of the Real Estate to permit construction of single-family residential units as set out below. If Buyer is not completely satisfied with the Real Estate to its sole satisfaction at any such time during the Rezoning Period, Buyer may terminate this Agreement for any and all reason(s) by delivering notice to Seller on or before the expiration of the Rezoning Period, and the Deposit (defined below in Section 3) shall be handled per Section 3 of this Agreement. Buyer will use its best efforts its best efforts to timely, actively and diligently pursue rezoning of the Real Estate. Seller shall fully cooperate with Buyer in doing so. Buyer may elect to extend the Rezoning Period by making said election and providing written notice to Seller of same prior to the expiration of the then current period as described herein:
 - a. **Rezoning Period.** The Rezoning Period shall commence upon the Effective Date and shall expire at midnight on May 30, 2022 ("Rezoning Period").
 - b. **Rezoning Period Extension No. 1.** Rezoning Period Extension No. 1 shall commence upon the expiration date of the Rezoning Period and shall expire at midnight on July 4, 2022 ("Rezoning Period Extension No. 1").
 - c. **Rezoning Period Extension No. 2.** Rezoning Period Extension No. 2 shall commence upon the expiration date of the Rezoning Period Extension No. 1 and shall expire at midnight on August 29, 2022 ("Rezoning Period Extension No. 2").
3. **EARNEST MONEY DEPOSIT.** Buyer has deposited \$_____ ("Review Deposit") in escrow per the escrow agreement attached hereto as **Exhibit C** ("LOI Escrow Agreement"). By 5 business days from the Effective Date and upon execution of the escrow agreement attached hereto as **Exhibit D** ("Escrow Agreement"), the LOI Escrow Agreement shall terminate, Escrow Agent shall close the escrow account established pursuant to the LOI Escrow Agreement, shall transfer such Review Deposit into the escrow account as established by the Escrow Agreement, and Buyer shall deliver to the Escrow Agent to be held in escrow per the Escrow Agreement an additional earnest money

Rezoning Period, Rezoning Period Extension No. 1 and Rezoning Period Extension No. 2 collectively referred to herein as "Rezoning Period."

Jan 12, 2021
T.C. 12/20/20
M.L.C. 12-20-21

as a draft is available. Buyer shall select the exact number of acres, boundary lines and orientation of the Real Estate in its sole discretion to be reflected in the Survey.



8. **PLAN APPROVALS.** During the Rezoning Period or any extension thereof, Buyer may apply for certain plan approvals for the development of the Real Estate as a residential community, at Buyer's expense. Seller grants to Buyer the right to develop and present plans that include the Real Estate for zoning, subdivision and other development approvals. Seller also grants to Buyer the right to receive, accept and agree to zoning and other development approvals and permits. Seller shall cooperate with Buyer and execute any necessary applications or documents required for Buyer to receive such approvals and permits. Buyer agrees to give Seller copies of all plans prior to submitting for rezoning approvals.

9. **LICENSE/EASEMENTS/ACCESS.**

- a. **Buyer License.** Upon the Effective Date, Seller grants to Buyer a non-exclusive right of way and license in, on, over, under and across the Real Estate to conduct its review of the Real Estate, including but not limited to engineering work, geotechnical analysis and collection of other necessary data for development ("License"). In exercising its License, Buyer shall not cause permanent damage to the Real Estate and shall restore any disturbed areas to the pre-damage condition. Also, Buyer shall indemnify and hold Seller harmless from any and all obligations, claims, demands, liens or encumbrances, including costs and expenses and attorney fees, arising from any acts or omissions of Buyer, its agents, servants and employees, in exercising its License rights. Notwithstanding the foregoing, such indemnification shall not extend to the discovery or disturbance of pre-existing hazardous materials (defined below in Section 11). Buyer agrees to share with Seller all studies, reports or plans created by Buyer during the contract period.
- b. **Buyer Easements.** Upon the Effective Date, Seller shall execute all rights of way and easement documents reasonably requested by Buyer to effectuate the intent of this Agreement ("Easements"). Such Easements shall be on Buyer's form and at Buyer's expense.

10. **IMPROVEMENTS/RISK OF LOSS.** Until Closing and transfer of possession of the Real Estate, Seller shall maintain the Real Estate and any improvements thereon in substantially the same condition existing as of the Effective Date. All improvements to the Real Estate including any buildings or structures thereon are included in the value and Purchase Price. The risk of loss to the Real Estate and any improvements thereon by fire, natural causes or otherwise prior to Closing is that of Seller. Seller shall provide insurance coverage for the full value of the Real Estate and improvements until Closing. Upon Buyer's request, Seller shall immediately deliver to Buyer a copy of same.

11. **SELLER REPRESENTATIONS AND WARRANTIES.** Seller agrees to the following representations and warranties regarding any portion of the Real Estate as of the Effective Date and Closing:

- a. **Authority.** Seller's execution of this Agreement and the consummation of the transaction contemplated herein are within Seller's authority and capacity and all requisite action(s) have occurred to make this Agreement a valid and binding obligation of Seller.
- b. **Other Agreements.** There are no material undisclosed, unrecorded agreements or understandings to which Seller is a party affecting any portion of the Real Estate, which will be binding upon Buyer or the Real Estate after Closing. Also, Seller's execution of this Agreement and the consummation of the transaction contemplated herein do not and will not result in a breach of or default under any indenture, agreement, instrument or obligation to which Seller is a party and which affects any portion of the Real Estate, or violate any applicable law.

IN WITNESS THEREOF, the Parties have executed this Agreement on the date indicated below.

SELLER: TIN CHAN and MIU LIN CHAN, a married couple

Tin Chan
By: Tin Chan
Date:

Witness: [Signature]

Miu Lin Chan
By: Miu Lin Chan
Date:

Witness: [Signature]

SELLER: DANNY ENG and SHUN NGAN ENG, a married couple

[Signature]
By: Danny Eng
Date: 12-13-2021

Witness: [Signature]

[Signature]
By: Shun Ngan Eng
Date: 12-13-2021

Witness: [Signature]

BUYER: GRAND COMMUNITIES, LLC, a Kentucky limited liability company

[Signature]
By: Todd E. Huss
Its: President
Date: 12/20/2021

Witness: [Signature]



Memorandum

To: Kenneth Wood, Planners and Engineers Collaborative, Inc.
From: Abdul Amer, PE
Date: June 29th, 2022
Subject: Trip Generation Memorandum for Proposed Residential Development located at 2325 SR 120 (Old Milton Parkway), City of Alpharetta, Georgia – A&R Project #22-137



The purpose of this memorandum is to estimate the trip generation from the residential development proposed along SR 120 (Old Milton Parkway) in City of Alpharetta, Georgia. The proposed development will consist of 24 units of single-family attached housing.

A site plan is attached and a site overlay is shown below.

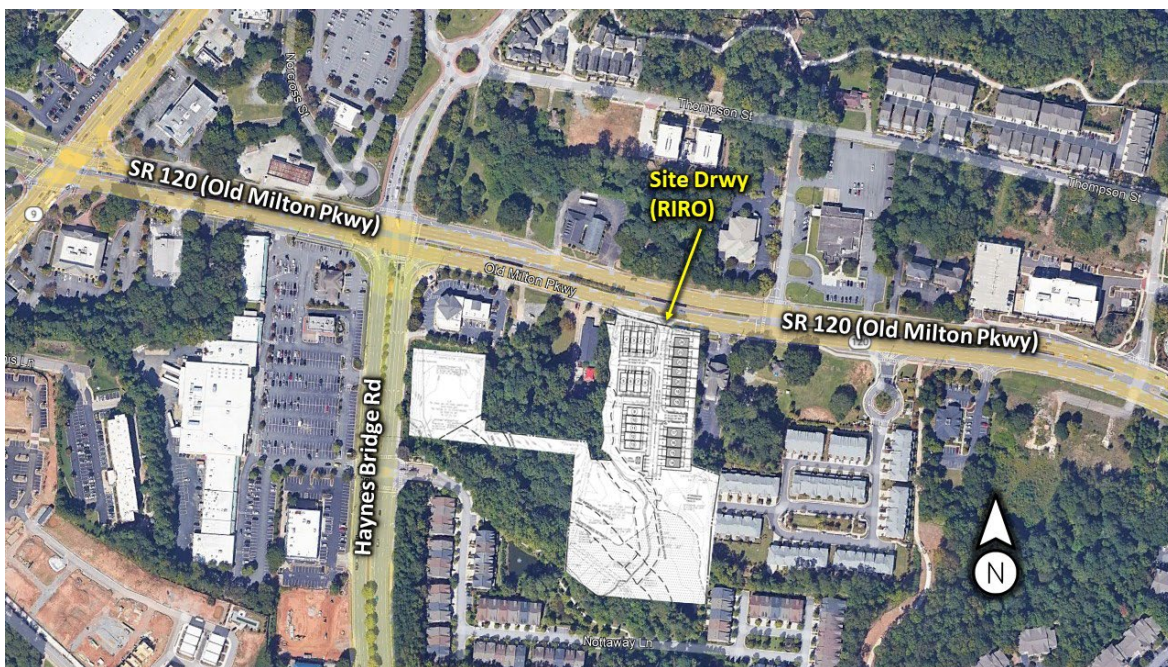


Figure 1 - Site Overlay Map

METHODOLOGY

Trip generation estimates for the project were based on the rates and equations published in the 11th edition of the Institute of Transportation Engineers (ITE) Trip Generation Manual. This reference contains traffic volume count data collected at similar facilities nationwide. The trip generation referenced is based on the following ITE Land Uses: 215 – *Single-Family Attached Housing*.

Land Use: 215 – Single-Family Attached Housing: Single-family attached housing includes any single-family housing unit that shares a wall with an adjoining dwelling unit, whether the walls are for living space, a vehicle garage, or storage space.



A&R Engineering, Inc.

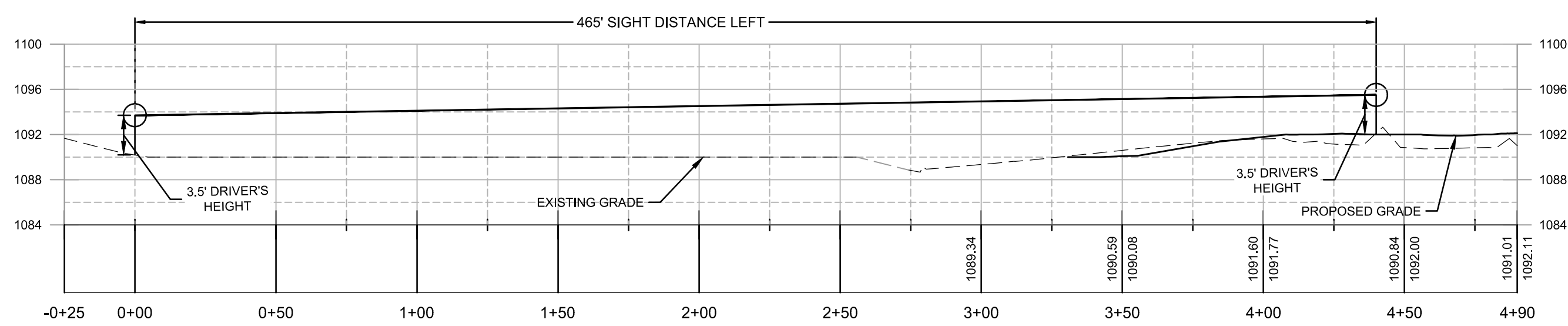
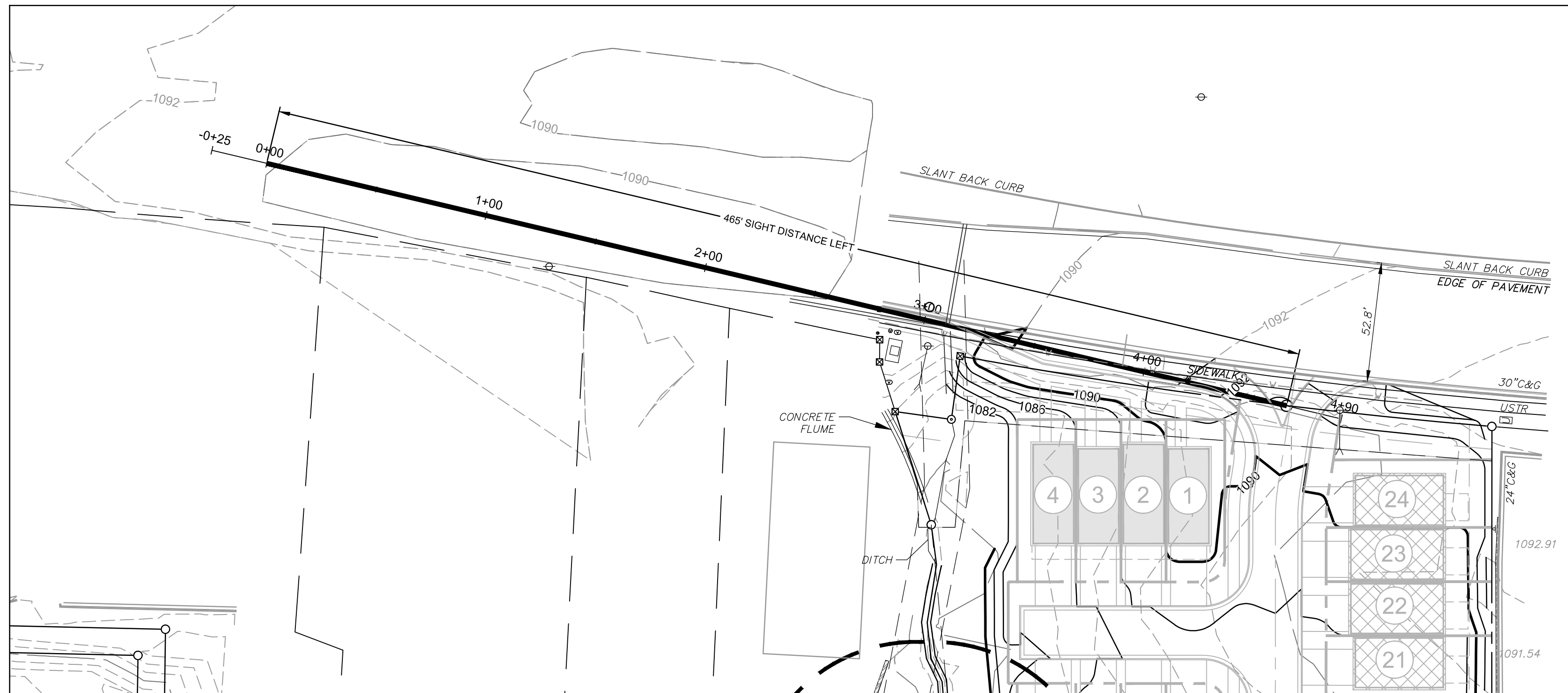
TRIP GENERATION

The results of the analysis for the proposed development are shown in Table 1, below.

Table 1 – Trip Generation								
Land Use	Size	AM Peak Hour			PM Peak Hour			24 Hour
		Enter	Exit	Total	Enter	Exit	Total	Two-way
ITE 215 – Single-Family Attached Housing	24 units	2	5	7	5	5	10	132

Based on the trip generation rates published in Institute of Transportation Engineer's Trip Generation Manual, 11th Edition, the proposed development will generate 2 entering trips and 5 exiting trips in the AM peak hour and 5 entering trips and 5 exiting trips in the PM peak hour.

APPENDIX



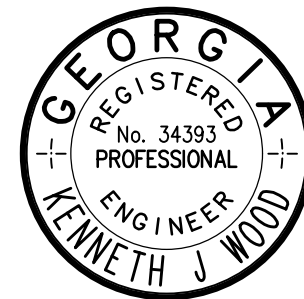
SIGHT DISTANCE PROFILE
HORIZONTAL SCALE: 1" = 40'
VERTICAL SCALE: 1" = 10'

SIGHT DISTANCE NOTES:

1. SPEED LIMIT ON ROAD NAME IS XX MPH
2. ALL SIGNS AND PAVEMENT MARKINGS SHALL CONFORM TO THE "MANUAL ON UNIFORM TRAFFIC CONTROL DEVICES", (LATEST EDITION) AND ANY APPLICABLE ALPHARETTA STANDARDS.
3. ALL PAVEMENT MARKINGS WITHIN THE RIGHT OF WAY SHALL BE THERMOPLASTIC UNLESS OTHERWISE NOTED.
4. ALL TRAFFIC CONTROL DEVICES SHALL BE MAINTAINED BY THE CONTRACTOR SO AS NOT TO INTERFERE WITH SIGHT DISTANCE ALONG ANY ADJACENT SIDE ROAD OR DRIVEWAY.
5. THE CONTRACTOR SHALL MAINTAIN INGRESS AND EGRESS TO DRIVEWAYS AT ALL TIMES.
6. SIGHT DISTANCES WERE TAKEN FROM GEORGIA DEPARTMENT OF TRANSPORTATION REGULATIONS FOR DRIVEWAY AND ENCROACHMENT CONTROL, TABLE 3-4 (INTERSECTION SIGHT DISTANCE REQUIREMENTS).
7. OLD MILTON PARKWAY IS A DIVIDED HIGHWAY WITH 3 LANES TRAVELING LANES ON THE SIDE OF THE ROAD AS THE PROPOSED DEVELOPMENT. THE DEVELOPMENT WILL HAVE A RIGHT-IN, RIGHT-OUT ENTRANCE.

SIGHT DISTANCE CERTIFICATION:

1. THE UNDERSIGNED, HEREBY CERTIFY THAT THE PROPOSED ENTRANCE/EXIT
 ONTO OLD MILTON PKWY IS DESIGNED WITH ADEQUATE SIGHT DISTANCE.
 THE POSTED SPEED LIMIT OF OLD MILTON PKWY IS 45 MPH. THE INGRESS/EGRESS
 FOR THE PROPERTY WILL BE A RIGHT-IN, RIGHT-OUT ONLY, SO THE APPLICABLE
 SIGHT DISTANCE IS 465' SDL FOR A 3-LANE ROAD, AS REQUIRED BY THE
 FIVE-FOOT MINIMUM CLEARANCE, SIGHT DISTANCE IS ASSURED ALONG
 THE PATH OF TRAVEL AT A HEIGHT OF 3.5' ABOVE THE SURFACE OF
 THE ROADWAY. TO AN OBJECT ON THE CENTERLINE OF THE ROAD 3.5' ABOVE THE
 SURFACE OF THE ROADWAY.



DATE: 6/30/2022

P: (770) 451-2741 F: (770) 451-3915

WWW.PEC.PLUS



Planners & Engineers Collaborative+

LAND PLANNING + LANDSCAPE ARCHITECTURE + CIVIL ENGINEERING
ARBORISTS + SURVEYING & CONSTRUCTION + WATER RESOURCES

350 RESEARCH COURT STE 200
PEACHTREE CORNERS, GA 30092

PROJECT

2325 OLD MILTON

A MASTER PLANNED RESIDENTIAL
DEVELOPMENT

AT

2325 OLD MILTON
NORCROSS STREET
HAYNES BRIDGE ROAD

**CITY OF ALPHARETTA
JURISDICTION**

FOR

GRAND COMMUNITIES, LLC

MUNICIPALITY PROJECT #

REVISIONS

[illegible]

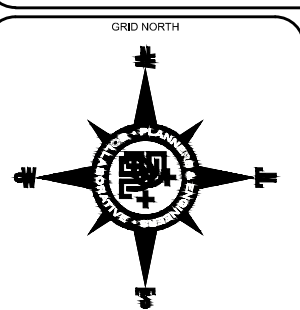
THIS SEAL IS ONLY VALID IF COUNTER SIGNED
AND DATED WITH AN ORIGINAL SIGNATURE.



SIGHT DISTANCE PROFILE



SCALE: 1" = 40'
DATE: 04/19/2022
PROJECT: 15315.01



SD1

SHEET





CITY COUNCIL MEETING STAFF REPORT

SUBMITTING DEPARTMENT: COMMUNITY DEVELOPMENT

SUBMITTED BY: KATHI COOK

DRAFTED BY: MICHAEL WOODMAN

CITY COUNCIL SPONSOR: STAFF INITIATED

I. **AGENDA ITEM TITLE:** PH-22-10 UNIFIED DEVELOPMENT CODE TEXT AMENDMENTS – BANNER SIGNS

CITY COUNCIL: SEPTEMBER 19, 2022

This item was considered at the 9/1/2022 Planning Commission meeting. There were no public comments. After discussion, Planning Commission recommended approval subject to changing 'retail and restaurant business' to 'commercial business' and adding the 'County' as it relates to roadway construction activities. Vote 7-0

II. **REPORT IN BRIEF:**

Consideration of text amendments to Unified Development Code (UDC) Section 2.6 Sign Code, to allow for an extension to the temporary banner permits for businesses fronting a roadway under construction by the city or the Georgia Department of Transportation.

DISCUSSION

The city's sign ordinance currently permits one banner per business for a 14-day period per calendar year or 2 banners with a 7-day maximum per calendar year. An amendment to the code is requested in order to provide the Director of Community Development authority, at the Director's sole discretion, to administratively allow a banner to remain past the 14-day period for a business that fronts a roadway that is under construction. The roadway construction must be a project under construction for 6 months or longer and a project overseen by the city, Georgia Department of Transportation or Fulton County. Multi-tenant properties would only be allowed a single banner and if banners are not maintained in good condition, removal would be required.

This change would help businesses along Main Street currently being impacted by the Georgia Department of Transportation (GDOT).

ATTACHMENTS:

- UDC Strike Through and Underline Edits

SECTION 2.6 SIGNS¹

2.6.11 General provisions.

E. BANNERS. Banners require a permit and are permitted in all zoning districts pursuant to the following standards:

1. Banners shall be permitted for either one (1) fourteen (14) day period per calendar year per lot or two (2) seven (7) day periods per calendar year per lot. An individual banner permit may be divided into two (2) non-consecutive seven (7) day periods provided the dates are stated on the permit. However, in the case of lots which contain a shopping center (or strip shopping center) with multiple tenant spaces, each tenant space shall be allowed to erect or place a banner for either one (1) fourteen (14) day period per calendar year or two (2) seven (7) day periods per calendar year.

a. The Director may grant an extension of the time period set forth above for a commercial business when the business fronts a roadway that is under construction. In order to qualify for such an extension:

1. The subject roadway construction must be related to a project performed by the City, County or the Georgia Department of Transportation; and
2. The subject roadway construction is planned to continue for three (3) months or more following the date of the request for an extension; and
3. The subject roadway construction either:
 - a. Causes the removal of a monument sign; or
 - b. As determined in the discretion of the Director, disrupts the store frontage to the extent the site and/or business appears closed without the use of a banner.

Any extension granted under this subsection shall be limited to the duration of the subject roadway construction. Extensions granted by the Director may be revoked or limited at any time due to changes in the roadway construction or disruption of the store frontage as determined in the discretion of the Director. The Director may require removal or replacement of any banner placed pursuant to an extension at any time if the banner is not maintained in good condition as determined in the discretion of the Director.

2. In addition to the foregoing, banners shall be allowed on private property during an approved temporary use, as defined in Section 2.3.2 of the U.D.C., for the approved period of such temporary use, but not to exceed forty-five (45) days; provided, however, the placement of banners on lots during approved temporary uses shall not be permitted more than two (2) times per calendar year per lot. Any such banners shall be removed upon termination of the temporary use or within forty-five (45) days from the date it is first placed on the lot, whichever is first to occur. Upon removal, no banner shall be placed on the same lot for a period of sixty (60) days.
3. Banners shall not exceed 24 sq. ft. total area in size.

¹Editor's note(s)—Ord. No. 720 , § 2(Exh. A), adopted 2-22-2016, repealed former § 2.6 (2.6.1—2.6.14), and enacted a new § 2.6 as set out herein. The former § 2.6 pertained to similar subject matter and derived from the original codification and Ord. No. 713 , §§ 1—8, adopted Sept. 28, 2015.

-
4. Banners must either be free-standing or mounted to the wall of a tenant space or the lot's existing monument sign. If free-standing, the height of the banner shall not exceed five (5) [feet] above grade. If mounted to the wall of a tenant space, the width of the banner shall not exceed tenant frontage and shall not extend above the horizontal plane of the roof where the building wall and roof meet. If mounted to the lot's existing monument sign, the banner shall not extend beyond the sign face of the monument sign.
 5. Banners shall be erected with supports or other means so that they do not sag or become dilapidated.
- F. PLACEMENT OF SIGNS. Except within the Central Business District, all free-standing signs must be set back at least ten (10) ft. from the public right-of-way. Within the Central Business District, all free standing signs must be set back at least five (5) feet from the public right-of-way.
- G. CHANGEABLE COPY. Any monument sign permitted under this Ordinance may contain up to sixty-five percent (65%) changeable copy if the sign is located on a lot zoned and used (as its principal existing use) for an institutional, public or semi-public use and which includes an indoor public assembly place accommodating one hundred (100) or more persons.

(Ord. No. 720 , § 2(Exh. A), 2-22-2016)

AN ORDINANCE TO AMEND ARTICLE II OF THE UNIFIED DEVELOPMENT CODE OF THE CITY OF ALPHARETTA, GEORGIA; TO AMEND REGULATIONS PERTAINING TO BANNER SIGNS; TO REPEAL CONFLICTING ORDINANCES; AND FOR OTHER PURPOSES.

WHEREAS, on or about May 21, 2001, the City of Alpharetta (the “City”) adopted a comprehensive zoning ordinance known and cited as the Unified Development Code of the City of Alpharetta, Georgia, which has subsequently been amended from time to time (the “Unified Development Code”); and

WHEREAS, the Mayor and Council of the City of Alpharetta (the “City Council” or “Council”) are charged with the protection of the public health, safety, and welfare of the citizens of the City of Alpharetta; and

WHEREAS, the Unified Development Code was designed to be amended from time to time when circumstances warrant that modifications be made in order to make said Codes more responsive to community needs; and

WHEREAS, the City Council finds that ordinances and regulations governing the uses of land and development of land within the City, as well as the City’s operations, should be continually improved from time to time and modified as necessary to better protect and promote the public health, safety and welfare of the residents and businesses of the City of Alpharetta; and

WHEREAS, the City Council desires to amend Article II of the Unified Development Code for the foregoing purposes; and

WHEREAS, the City Council finds that the following amendments to the Unified Development Code promote the health, safety, morals, convenience, order, prosperity and general welfare of the present and future inhabitants of the City of Alpharetta;

NOW THEREFORE, The Council of the City of Alpharetta hereby ordains, as follows:

Section 1: Article II, Subsection 2.6.11(E) titled “Banners” of the Unified Development Code is hereby amended by revising same as set forth in Exhibit “A” attached hereto as if fully set forth herein.

Section 2: If any section, subsection, provisions, or clause of any part of this Ordinance shall be declared invalid or unconstitutional or, if the provisions of any part of this Ordinance as applied to any particular situation or set of circumstances shall be declared invalid or unconstitutional, such invalidity shall not be construed to affect the portions of this Ordinance not so held to be invalid, or the application of this Ordinance to other circumstances not so held to be invalid. It is hereby declared as the intent of the City Council that this Ordinance would have been adopted in its current form without the invalid or unconstitutional provision contained therein.

Section 3: This Ordinance shall be effective immediately upon its adoption by the City Council and the amendments made herein shall be incorporated into the Unified Development Code of the City of Alpharetta, Georgia, as applicable. This Ordinance hereby repeals any and all conflicting ordinances and amendments.

SO ORDAINED this the _____ day of _____, 2022.

Approved:

Jim Gilvin, Mayor

Attest:

Lauren Shapiro, City Clerk
(Seal)

Approved as to Form:

City Attorney

COUNCILMEMBERS

Exhibit “A”

SECTION 2.6 SIGNS¹

2.6.11 General provisions.

E. BANNERS. Banners require a permit and are permitted in all zoning districts pursuant to the following standards:

1. Banners shall be permitted for either one (1) fourteen (14) day period per calendar year per lot or two (2) seven (7) day periods per calendar year per lot. An individual banner permit may be divided into two (2) non-consecutive seven (7) day periods provided the dates are stated on the permit. However, in the case of lots which contain a shopping center (or strip shopping center) with multiple tenant spaces, each tenant space shall be allowed to erect or place a banner for either one (1) fourteen (14) day period per calendar year or two (2) seven (7) day periods per calendar year.

a. The Director may grant an extension of the time period set forth above for a commercial business when the business fronts a roadway that is under construction. In order to qualify for such an extension:

1. The subject roadway construction must be related to a project performed by the City, County or the Georgia Department of Transportation; and
2. The subject roadway construction is planned to continue for three (3) months or more following the date of the request for an extension; and
3. The subject roadway construction either:
 - a. Causes the removal of a monument sign; or
 - b. As determined in the discretion of the Director, disrupts the store frontage to the extent the site and/or business appears closed without the use of a banner.

Any extension granted under this subsection shall be limited to the duration of the subject roadway construction. Extensions granted by the Director may be revoked or limited at any time due to changes in the roadway construction or disruption of the store frontage as determined in the discretion of the Director. The Director may require removal or replacement of any banner placed pursuant to an extension at any time if the banner is not maintained in good condition as determined in the discretion of the Director.

2. In addition to the foregoing, banners shall be allowed on private property during an approved temporary use, as defined in Section 2.3.2 of the U.D.C., for the approved period of such temporary use, but not to exceed forty-five (45) days; provided, however, the placement of banners on lots during approved temporary uses shall not be permitted more than two (2) times per calendar year per lot. Any such banners shall be removed upon termination of the temporary use or within forty-five (45) days from the date it is first placed on the lot, whichever is first to occur. Upon removal, no banner shall be placed on the same lot for a period of sixty (60) days.
3. Banners shall not exceed 24 sq. ft. total area in size.
4. Banners must either be free-standing or mounted to the wall of a tenant space or the lot's existing monument sign. If free-standing, the height of the banner shall not exceed

¹Editor's note(s)—Ord. No. 720 , § 2(Exh. A), adopted 2-22-2016, repealed former § 2.6 (2.6.1—2.6.14), and enacted a new § 2.6 as set out herein. The former § 2.6 pertained to similar subject matter and derived from the original codification and Ord. No. 713 , §§ 1—8, adopted Sept. 28, 2015.

five (5) [feet] above grade. If mounted to the wall of a tenant space, the width of the banner shall not exceed tenant frontage and shall not extend above the horizontal plane of the roof where the building wall and roof meet. If mounted to the lot's existing monument sign, the banner shall not extend beyond the sign face of the monument sign.

5. Banners shall be erected with supports or other means so that they do not sag or become dilapidated.
- F. **PLACEMENT OF SIGNS.** Except within the Central Business District, all free-standing signs must be set back at least ten (10) ft. from the public right-of-way. Within the Central Business District, all free standing signs must be set back at least five (5) feet from the public right-of-way.
- G. **CHANGEABLE COPY.** Any monument sign permitted under this Ordinance may contain up to sixty-five percent (65%) changeable copy if the sign is located on a lot zoned and used (as its principal existing use) for an institutional, public or semi-public use and which includes an indoor public assembly place accommodating one hundred (100) or more persons.

(Ord. No. 720 , § 2(Exh. A), 2-22-2016)



STAFF REPORT

Submitting Department: Public Works

Submitted By: Arash Moradkhani

Sponsored By:

Meeting Date: September 26, 2022

I. AGENDA ITEM TITLE: DESIGN SERVICES: PEDESTRIAN SAFETY IMPROVEMENTS (RFQ 22-1007) APPROVAL OF THE AWARD OF RFQ 22-1007 (PEDESTRIAN SAFETY IMPROVEMENT DESIGN SERVICES) AND ROSWELL STREET ALPHA LOOP DESIGN SERVICES (OLD MILTON PARKWAY TO OLD ROSWELL STREET) TO MOFFATT & NICHOL.

II. RECOMMENDATION:

Please award RFQ 22-1007 (Pedestrian Safety Improvement design services) and Roswell Street Alpha Loop design services (Old Milton Pkwy to Old Roswell Street) to Moffatt & Nichol in an amount totaling \$272,000.00 and authorize the Mayor to execute all necessary documents.

III. BUDGET IMPLICATIONS:

BUDGETED ITEM: YES

FISCAL IMPACT: YES

INCLUDED IN CURRENT FY CPTL BUDGET: YES

INCLUDED IN CURRENT FY OPRT. BUDGET: NO

TOTAL PROJECT COST: \$272,00.00

APPROPRIATIONS:

<u>ACCOUNT TITLE/NUMBER</u>	<u>DOLLAR AMOUNT</u>
Marietta St at Roswell St Safety Improvements (TSPLOST 2; 33641100-541410-C2224)	\$140,000.00
Improved Ped Crossings from City Center to Churches (TSPLOST 2; 33641100-541410-C2225)	\$102,500.00
Pedestrian Safety Barrier at City Center (30161150-541500-C2030)	\$29,500.00

EXTERNAL FUNDING SOURCES:

<u>ACCOUNT TITLE/NUMBER</u>	<u>DOLLAR AMOUNT</u>
NA	\$0.00
NA	\$0.00
N/A	\$0.00

IV. REPORT IN BRIEF:

The award of this project is for design services associated with pedestrian safety and connectivity improvements in the Downtown Area.

A scoping document was prepared for the following four projects by the Public Works Department and an RFQ (Request for Qualifications) was issued on June 16, 2022.

1. Roswell Street at Marietta Street Intersection

This proposed project is to review the intersection of Roswell Street at Marietta Street for safety improvements that would reduce vehicle speeds, improve visibility, shorten the distance to cross the street, and provide pedestrian refuges. Roswell Street, between Old Roswell Street and Old Milton Parkway, will be comprehensively studied to determine the most optimum safety treatment at the intersection of Roswell Street and Marietta Street.

2. Academy Street at City Center

This proposed project is to review the section of Academy Street from Highway 9 to Haynes Bridge Road for improvements that would reduce vehicle speeds, improve visibility, shorten the distance pedestrians must traverse to cross the street, and provide pedestrian refuge.

3. Wall Design on Highway 9 from South Broad Street to North Broad Street

This proposed project is to design street walls along the sidewalk on Highway 9 in front of the Town Green so as to improve safety. Three walls are proposed for this project. All three walls will be veneered (both sides) with brick to match City Hall and will have a capstone similar to the ones within the City Center. We are looking into two options for the walls' height; 18 inches and 36 inches.

4. Self-Standing Outdoor Kiosk

This would be to study the Downtown Area along Highway 9 and design a self-standing, outdoor kiosk at an optimum location to promote residents' and visitors' information about the city. All necessary components for the safe and efficient operation of the kiosk such as fiber optic cable, remote communication routers, and power connection will be included in the design and construction plans. The kiosk will be waterproof and dust-proof with a preferred height of 80 inches.

A total of five responses to the RFQ were received on July 14, 2022.

Staff from the Public Works Department evaluated and scored the proposals based on the design team's: experience and qualifications (40%); references (20%); and quality of completed project examples (40%). The final scoring, out of 100, based on qualifications was:

- Keck & Wood, Inc. (84)
- Croy Engineering, LLC (81)
- Columbia Engineering (78.50)
- Moffatt & Nichol (77)
- Axis Infrastructure, LLC (76.50)

All five consultants were invited for in-person meetings and interviews with the Public Works Department on August 8-9, 2022 to further evaluate their understanding of our projects and design approach. The final scoring, out of 100, based on interviews was:

- Moffatt & Nichol (93.33)
- Croy Engineering, LLC (90)
- Columbia Engineering (66.67)
- Axis Infrastructure, LLC (66.67)
- Keck & Wood, Inc. (60)

The final combined scoring, out of 200, based on qualifications and interviews is:

- Croy Engineering, LLC (171)
- Moffatt & Nichol (170.33)
- Columbia Engineering (145.17)
- Keck & Wood, Inc. (144)
- Axis Infrastructure, LLC (143.17)

Preliminary Cost Submission based on scope detailed in RFQ 22-1007

Based on the final scoring for qualifications and interviews, staff requested cost proposals from the top 2 scoring firms: Croy Engineering; and Moffatt & Nichol. Results were as follows:

- Moffatt & Nichol: \$200,000
- Croy Engineering, LLC: \$395,686

The project approach was vastly different between the two firms. For example, Croy's proposal included a far more in-depth public outreach component and the cost estimate for the work along Academy Street was five times the cost of the proposal from Moffat and Nichol. Moffat and Nichol utilized the adopted downtown pedestrian plan as the basis of the work along Academy Street and at the intersection of Marietta and Roswell Street (refer to attached exhibits).

Additional Scope Item: Roswell Street Alpha Loop

The Community Development Department received the Downtown Link Alpha Loop study. As a part of this study, wider sidewalks are recommended to be designed and constructed along Roswell Street between Old Milton Pkwy and Old Roswell Street. Although the study has not been adopted at this time, staff requested Moffatt & Nichol to add a separate line item to their cost proposal for the future design of Roswell Street Alpha Loop from Old Milton Parkway to Old Roswell Street. This is to ensure that safety improvements at the intersection of Roswell Street & Marietta Street would not contradict the Alpha Loop design along Roswell Street. If the Roswell Street Alpha Loop design does not become necessary, Moffatt & Nichol would not charge for that line item.

Final Cost Submission including the Additional Scope detailed above

The total design cost of the following five projects from Moffatt & Nichol is \$272,000.00 and attached hereto as well as synopsized below:

- Roswell Street at Marietta Street intersection (\$65,500);
- Academy Street at City Center (\$100,000);
- Wall Design on Highway 9 from South Broad Street to North Broad Street (\$20,500);
- Self-Standing Outdoor Kiosk (\$6,500);
- Roswell Street Alpha Loop (\$72,000); and
- Public Involvement/Stakeholder Meetings (\$7,500).

Public Works staff met with Moffat and Nichol to discuss their proposal and expectations of the City. Moffat and Nichol confirmed their cost proposal will cover the necessary costs to design the pedestrian improvements. Moffatt & Nichol is an experienced firm that has worked on similar design projects throughout the metro Atlanta area. Once a contract with Moffatt & Nichol is finalized and executed, design work will begin immediately. The anticipated completion date of all five design projects is 17 months from the notice to proceed.

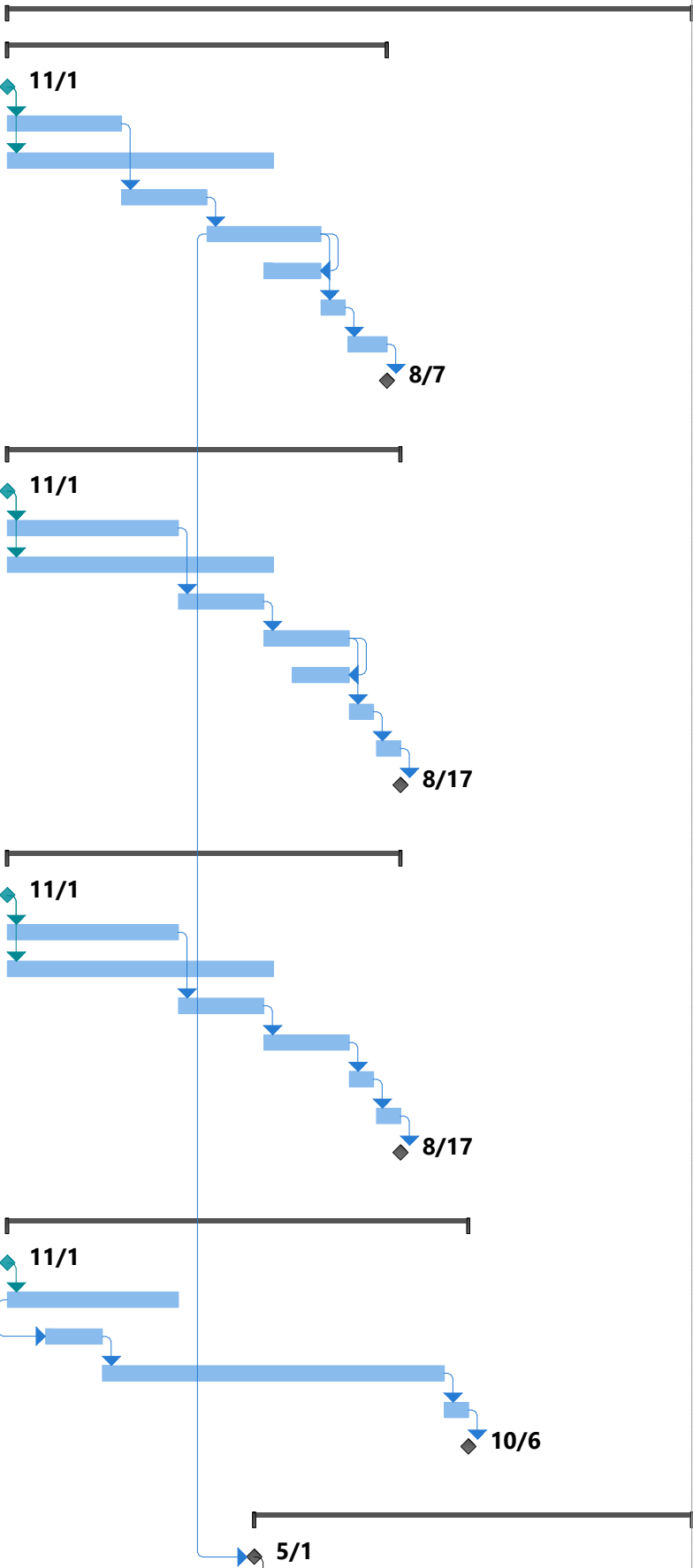
V. ALTERNATIVES:

None.

VI. ATTACHMENTS:

MoffattNichol_Projects Schedule, Academy St Mid-Block by Churches, Roswell at Marietta St Rasied Intersection, Moffat and Nichol's Proposal, RFQ 22-1007 Statement of Qualifications June 7 2022, RFQ 22-1007 Design Services Pedestrian Imp- Record of Receipt

ID		Task Mode	Task Name	Duration	Start	Finish	Predecessors	2, 2022							Half 1, 2023					Half 2, 2023					Half 1, 2024				
								A	S	O	N	D	J	F	M	A	M	J	J	A	S	O	N	D	J	F	M	A	M
1			Design Services- Pedestrian Safety Improvements	361 days	Tue 11/1/22	Tue 3/19/24																							
2			1- Roswell Street at Marietta Street Intersection	200 days	Tue 11/1/22	Mon 8/7/23																							
3			NTP	0 days	Tue 11/1/22	Tue 11/1/22																							
4			Topographical Field Survey	60 days	Tue 11/1/22	Mon 1/23/23	3																						
5			Utility Coordination	140 days	Tue 11/1/22	Mon 5/15/23	3																						
6			Concept Design and coordination with City	45 days	Tue 1/24/23	Mon 3/27/23	4																						
7			Final intersection design	60 days	Tue 3/28/23	Mon 6/19/23	6																						
8			Lighting study and design	30 days	Tue 5/9/23	Mon 6/19/23	7FF																						
9			Plan review by City	14 days	Tue 6/20/23	Fri 7/7/23	7																						
10			Address City Comments and Prepare and submit final plans for bidding	21 days	Mon 7/10/23	Mon 8/7/23	9																						
11			Submit the bidding package to City	0 days	Mon 8/7/23	Mon 8/7/23	10																						
12																													
13			2- Academy Street at City Center	208 days	Tue 11/1/22	Thu 8/17/23																							
14			NTP	0 days	Tue 11/1/22	Tue 11/1/22																							
15			Topographical Field Survey	90 days	Tue 11/1/22	Mon 3/6/23	14																						
16			Utility Coordination	140 days	Tue 11/1/22	Mon 5/15/23	14																						
17			Concept Design and coordination with City	45 days	Tue 3/7/23	Mon 5/8/23	15																						
18			Final design	45 days	Tue 5/9/23	Mon 7/10/23	17																						
19			Landscape design	30 days	Tue 5/30/23	Mon 7/10/23	18FF																						
20			Plan review by City	14 days	Tue 7/11/23	Fri 7/28/23	18																						
21			Address City Comments and Prepare and submit final plans for bidding	14 days	Mon 7/31/23	Thu 8/17/23	20																						
22			Submit the bidding package to City	0 days	Thu 8/17/23	Thu 8/17/23	21																						
23																													
24			3- Wall Design on HWY 9 from S. Broad St. to N. Broad St.	208 days	Tue 11/1/22	Thu 8/17/23																							
25			NTP	0 days	Tue 11/1/22	Tue 11/1/22																							
26			Topographical Field Survey	90 days	Tue 11/1/22	Mon 3/6/23	25																						
27			Utility Coordination	140 days	Tue 11/1/22	Mon 5/15/23	25																						
28			Concept Design and coordination with City	45 days	Tue 3/7/23	Mon 5/8/23	26																						
29			Final wall design	45 days	Tue 5/9/23	Mon 7/10/23	28																						
30			Plan review by City	14 days	Tue 7/11/23	Fri 7/28/23	29																						
31			Address City Comments and Prepare and submit final plans for bidding	14 days	Mon 7/31/23	Thu 8/17/23	30																						
32			Submit the bidding package to City	0 days	Thu 8/17/23	Thu 8/17/23	31																						
33																													
34			4- Self-standing Outdoor Kiosk	244 days	Tue 11/1/22	Fri 10/6/23																							
35			NTP	0 days	Tue 11/1/22	Tue 11/1/22																							
36			SUE investigation /designation and coordination with utility companies	90 days	Tue 11/1/22	Mon 3/6/23	35																						
37			Kiosk concept design	30 days	Tue 11/29/22	Mon 1/9/23	36SS+20 days																						
38			Kiosk final design and manufacturing	180 days	Tue 1/10/23	Mon 9/18/23	37																						
39			Prepare and submit final plans for bidding	14 days	Tue 9/19/23	Fri 10/6/23	38																						
40			Submit the bidding package to City	0 days	Fri 10/6/23	Fri 10/6/23	39																						
41																													
42			5- Roswell Street Alpha Loop from Old Milton to Old Roswell	231 days	Mon 5/1/23	Tue 3/19/24																							
43			NTP	0 days	Mon 5/1/23	Mon 5/1/23	7SS+25 days																						



ID		Task Mode	Task Name	Duration	Start	Finish	Predecessors	2, 2022					Half 1, 2023			Half 2, 2023					Half 1, 2024								
								A	S	O	N	D	J	F	M	A	M	J	J	A	S	O	N	D	J	F	M	A	M
44			Topographical Field Survey and SUE investigation	60 days	Tue 5/2/23	Mon 7/24/23	43																						
45			Concept trail design and coordination with City	50 days	Tue 7/25/23	Mon 10/2/23	44																						
46			Final design	100 days	Tue 10/3/23	Mon 2/19/24	45																						
47			Landscape design	45 days	Tue 12/19/23	Mon 2/19/24	46FF																						
48			Plan review by City	14 days	Tue 2/20/24	Fri 3/8/24	46																						
49			Address City Comments and Prepare and submit final plans for bidding	21 days	Tue 2/20/24	Tue 3/19/24	47																						
50			Submit the bidding package to City	0 days	Tue 3/19/24	Tue 3/19/24	49																						

3/19

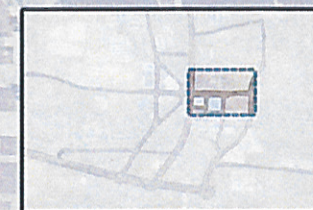


SITE OBSERVATIONS

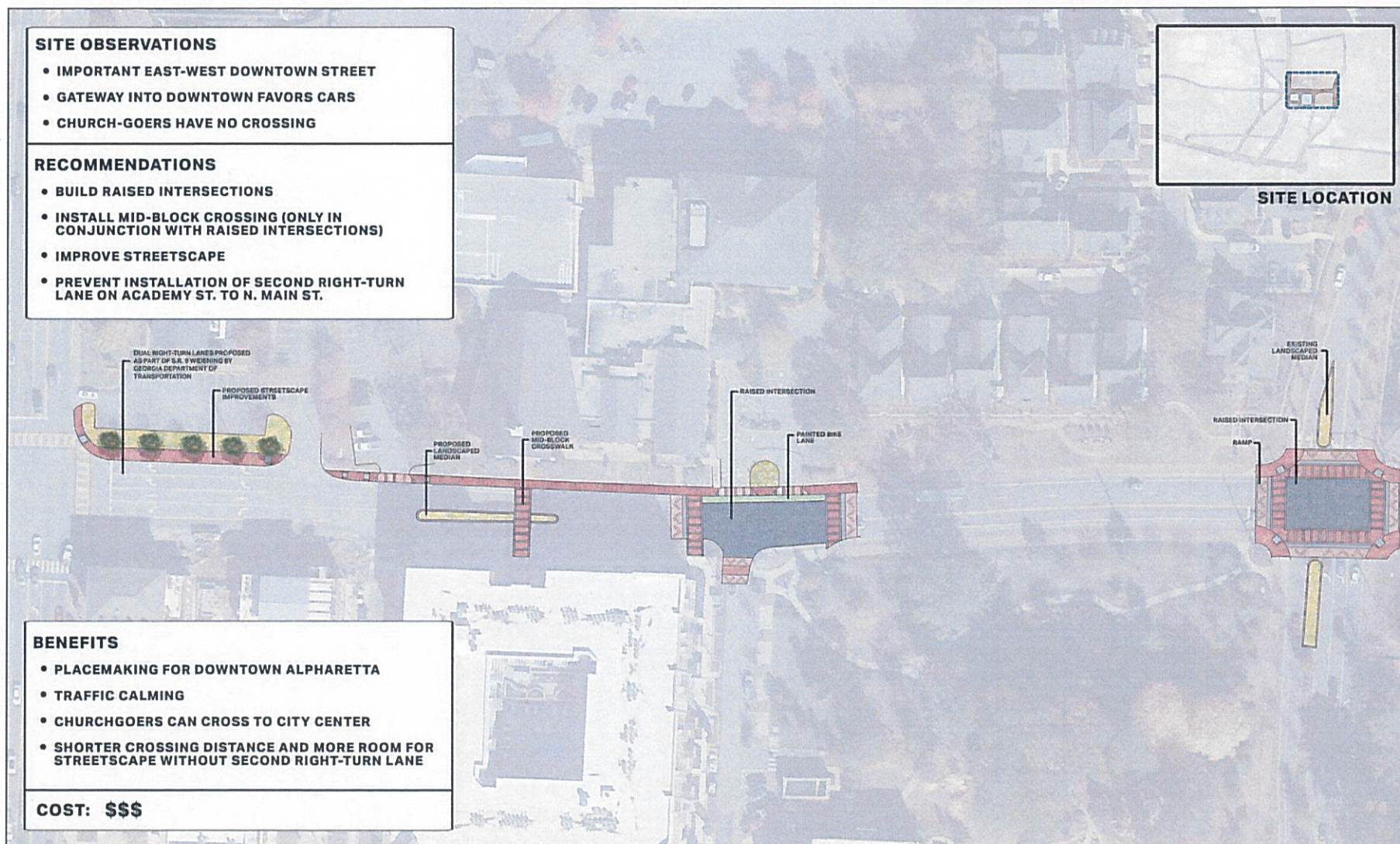
- IMPORTANT EAST-WEST DOWNTOWN STREET
- GATEWAY INTO DOWNTOWN FAVORS CARS
- CHURCH-GOERS HAVE NO CROSSING

RECOMMENDATIONS

- BUILD RAISED INTERSECTIONS
- INSTALL MID-BLOCK CROSSING (ONLY IN CONJUNCTION WITH RAISED INTERSECTIONS)
- IMPROVE STREETScape
- PREVENT INSTALLATION OF SECOND RIGHT-TURN LANE ON ACADEMY ST. TO N. MAIN ST.



SITE LOCATION



BENEFITS

- PLACEMAKING FOR DOWNTOWN ALPHARETTA
- TRAFFIC CALMING
- CHURCHGOERS CAN CROSS TO CITY CENTER
- SHORTER CROSSING DISTANCE AND MORE ROOM FOR STREETScape WITHOUT SECOND RIGHT-TURN LANE

COST: \$\$\$

**SITE OBSERVATIONS**

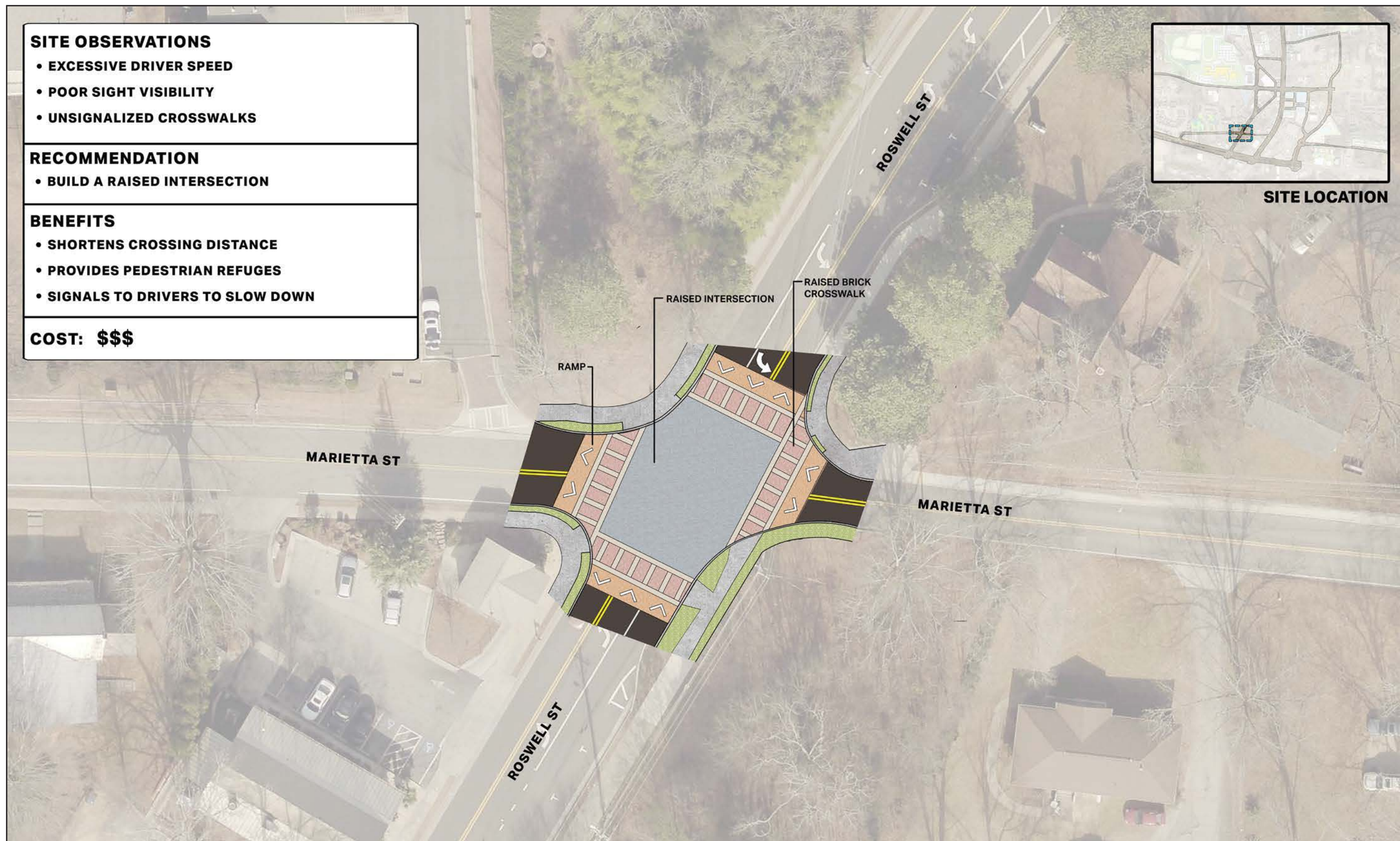
- EXCESSIVE DRIVER SPEED
- POOR SIGHT VISIBILITY
- UNSIGNALIZED CROSSWALKS

RECOMMENDATION

- BUILD A RAISED INTERSECTION

BENEFITS

- SHORTENS CROSSING DISTANCE
- PROVIDES PEDESTRIAN REFUGES
- SIGNALS TO DRIVERS TO SLOW DOWN

COST: \$\$\$**SITE LOCATION**

August 18, 2022

Ms. Debora Westbrook
Finance Department
2 Park Plaza
Alpharetta, GA 30009

**re: Design Services- Pedestrian Safety Improvements
Scope of Services and Engineering Budget Proposal
RFQ 22-1007**

Dear Debora,

Moffatt & Nichol is pleased to provide our proposed Scope of Services and Fee Proposal for providing professional engineering services to the City of Alpharetta on the Roswell Street at Marietta Street Intersection project, Academy Street at City Center project, Highway 9 from South Broad Street to North Broad Street project, Self-Standing Outdoor Kiosk, and Roswell Street Alpha Loop from Old Milton Pkwy to Old Roswell Street.

A. Roswell Street at Marietta Street Intersection

Prepare Concept and final construction plans*	\$45,000
Topographical field survey and utility coordination	\$10,500
Intersection Lighting study and design	\$8,000
Prepare detailed construction Cost estimates at 50%, 90%, and 100% plan submittal	\$2,000
Total Engineering Budget for Roswell Street at Marietta Street Intersection**	\$65,500

*Multiple design alternatives such as HAWK signal, raised intersection, raised concrete median, raised crossing, etc. will be considered. Roundabout design fee is not included in this estimate.

** Including the necessary information required for City to submit a NPDES Notice of Intent.

B. Academy Street at City Center

Prepare Concept and final construction plans	\$78,500
Topographical field survey and utility coordination	\$14,000
Landscape design	\$5,500
Prepare detailed construction Cost estimates at 50%, 90%, and 100% plan submittal	\$2,000
Total Engineering Budget for Academy Street at City Center**	\$100,000

* Multiple design alternatives such as HAWK signal, raised concrete median, raised crossing, etc. will be considered on Academy Street. Manning Street realignment survey and design is also part of this item.

**Including the necessary information required for City to submit a NPDES Notice of Intent.

C. Wall design on Highway 9 from South Broad Street to North Broad Street

Prepare Concept and final construction plans	\$7,000
Topographical field survey and SUE investigation/designation	\$12,500
Prepare detailed construction Cost estimates at 50%, 90%, and 100% plan submittal	\$1,000
Total Engineering Budget for Highway 9 from S. Broad Street to N. Broad Street*	\$20,500

*Including the necessary information required for City to submit a NPDES Notice of Intent.

D. Self-Standing Outdoor Kiosk

Prepare Concept and final construction plans	\$4,000
SUE investigation/designation & coordination with the utility companies	\$2,000
Prepare detailed construction Cost estimates at 50%, 90%, and 100% plan submittal	\$500
Total Engineering Budget for Academy Street at City Center	\$6,500*

*Including the necessary information required for City to submit a NPDES Notice of Intent.

E. Roswell Street Alpha Loop from Old Milton Pkwy to Old Roswell Street

Prepare Concept and final construction plans	\$65,000
Landscape design	\$5,000
Prepare detailed construction Cost estimates at 50%, 90%, and 100% plan submittal	\$2,000
Total Engineering Budget for Roswell Street Alpha Loop from Old Milton Pkwy to Old Roswell Street	\$72,000*

*Including the necessary information required for City to submit a NPDES Notice of Intent.

F. Public Involvement/Stakeholder Meetings **\$7,500**

Design Services for Pedestrian Safety Improvements- Total Cost: **\$272,000**

Additional Scope Items:

G. Construction Phase Services:

Assist the city with construction bid reviews, Request for Information (RFI), and Minor Plan Revisions	\$12,000
--	-----------------

The scope is based on the City of Alpharetta's RFQ 22-1007 and our understanding of the requirements to prepare engineering plans for these projects. Any items in the RFQ not listed here is not intentional and should be understood as services not included.

We appreciate this opportunity to partner with the City of Alpharetta and trust you will find that Moffatt & Nichol is a true partner that will serve with a focus on the City's best interests. We look forward to working with you and your staff. Please let me know if you need any additional information.

Sincerely,

MOFFATT & NICHOL

Fahim Attar, PE
Project Manager



CITY OF ALPHARETTA REQUEST FOR QUALIFICATIONS (RFQ)

RFQ Number: 22-1007

RFQ Title: Design Services: Pedestrian Safety Improvements

RFQ STATEMENT OF QUALIFICATIONS AND SUBMITTAL INFORMATION

1. RFQ Period of No Communication

The 'no communication period' starts on the issue date of this RFQ begins **Thursday, June 16, 2022**, and lasts through follow-up proposal, until the City Council meeting for contract award (or until contract award, if this isn't required to go before council for approval).

Any person or company, their employees, representatives, agents, attorneys, etc. must not contact the City's elected officials or any City staff concerning this RFQ.

Contacting anyone other than the Procurement Agent named below for this RFQ during this time will be reason to remove a response from review.

2. Procurement Agent, Single Point of Contact

Debora Westbrook is the Procurement Agent and Single Point of Contact for this RFQ and is the only contact representing the City for this RFQ.

Enter all questions or comments using Opportunity Q&A tab at the Bonfire project web page.

You can reach Debora at 678-297-6052 or purchasing@alpharetta.ga.us.

City of Alpharetta
2 Park Plaza
Alpharetta, GA 30009
Attn: Debora Westbrook, Procurement Agent

3. RFQ Schedule of Events

1. **Response Close Date, Deadline for Submissions: July 14, 2022 at 10:00 am.** We may change this date during the RFQ process. We will post any change in an addendum. Review web page for addenda.
2. Link to Bonfire Project Web Page: <https://cityofalpharetta.bonfirehub.com/>
3. This project web page has the important dates and all project documents for this RFQ.
4. Enter all questions, comments, requests for information before the Questions Due Date using ☒ **Message – Opportunity Q&A** at the project web page.
5. In each question, clearly note the RFQ document and section that is in question.
6. We will share any changes or added information from the City by a written addendum. We will make the information available to the public on the project web page.
7. It is your responsibility to check the project web page for any addenda, added information, or other messages before finally uploading a response. You must respond using any updated information.

4. Our Review of Responses and Review Criteria:

1. The City will make investigations as we feel necessary to make sure of your ability to provide the supplies or perform the work or services detailed in this RFQ.
2. We will first review all Statement of Qualifications responses (SOQ) to be sure that each response has basic requirements and information.
3. Some scoring may simply be Pass/Fail. We may remove any SOQ from further evaluation if we note a 'Fail' for any required response.
4. The Review Team will only get correct responses for review and scoring.
5. We will use this review and scoring to create a shortlist of the top-scoring responses. We will invite the shortlisted firms to take part in our Request for Proposal (RFP) process.
6. We will review and score each response using the criteria and percentage weights below:

Evaluation Criteria	Maximum Points
Cover Letter, Statement of Qualifications, Project Staffing, Available Resources	40
References	20
Quality of completed project examples	40
Total Maximum point score	100

7. If the City desires, the highest scoring firms will be shortlisted and invited to participate in a second phase consisting of an interview and presentation. The scoring for this **Phase 2 will be 100 maximum points** for the presentation and interview. For shortlisted firms, Phase 2 evaluation will be stand-alone final scoring.
8. If the City elects to move forward with the Phase 2 evaluation, shortlisted firms will be notified by close of business on **Friday, July 22, 2022**. Interviews would be conducted between July 27th and July 29th.
9. In the event the City elects not to move forward with Phase 2, Phase 1 scoring will stand as the sole scoring criteria.
10. If the City is unable to complete negotiations with the highest scoring firm, the City will then move to the next high scoring firm for negotiations. An actual contract award is subject to successful cost negotiation with the successful consultant.

WHAT WE WANT TO DO

General Description

The City of Alpharetta is requesting qualifications from consultants for the design of pedestrian safety improvements at three locations and an outdoor kiosk in the Downtown. This includes, but not limited to design work from concept to final construction plans for each location. These projects will be locally funded. No federal or state funding is anticipated.

Roswell Street at Marietta Street Intersection

This proposed project would review the intersection of Roswell Street at Marietta Street for improvements that would reduce vehicle speeds, improve visibility, shorten the distance to cross the street and provide pedestrian refuges.

Roswell Street between Old Roswell Street and Old Milton Parkway may need to be comprehensively studied to determine the most optimum safety treatment at the intersection of Roswell Street and Marietta Street.

Academy Street at City Center

This proposed project would review the section of Academy Street from SR9 to Haynes Bridge Road for improvements that would reduce vehicle speeds, improve visibility, shorten the distance to cross the street and provide pedestrian refuges.

Highway 9 from South Broad Street to North Broad Street

This proposed project is to design street walls along Highway 9 in front of the Town Green, on the existing sidewalk. Three walls are proposed for this project, per the attached Location Map. All three walls will be veneered (both sides) with brick to match City Hall and will have a capstone similar to ones within City Center. We are looking into two options for the walls' height: 18" and 36".

Self-Standing Outdoor Kiosk

This would be to study the Downtown area along Highway 9 and design a self-standing outdoor kiosk at an optimum location to promote residents and visitors information of the city. All necessary components for safe and efficient operation of the kiosk such as fiber optic cable, remote communication routers, and power connection shall be included in the design and construction plans. Existing fiber optic cables are underground and actively serve remote communication to traffic lights in the Downtown. The kiosk shall be water-proof and dust-proof with a preferred height of 80".

Scope of Work

The design team shall be responsible for the preparation and permitting of all necessary plans and providing the City with assistance during construction. This shall include, at a minimum, the following tasks:

1. Design – The design team will be responsible for the preparation of all necessary construction and right of way plans, details, specifications, special provisions, and/or studies necessary to provide final bidding plans. Construction and right of way plans should consider staging of the existing intersection and roadway segments and the proposed pedestrian safety improvements during construction. The City will provide right of way acquisition services for these projects if required. The design team will also be responsible for preparing an Opinion of Probable Construction Cost (OPCC) and assisting the City in determining a reasonable construction duration. An OPCC should be provided at concept and final plans. If required, the design team shall also provide the necessary information required for the City to submit a NPDES Notice of Intent.
2. Permitting – The design team will be responsible for any applicable state or federal permitting. Public Works' staff will review the plans for compliance with City requirements and coordinate any relevant reviews with Community Development. Note that should the total disturbed acreage for the project be 1.0 acre or greater, the erosion control plans will need to be submitted to the Georgia Environmental Protection Division. Any permit fees shall be paid directly by the City of Alpharetta.
3. Construction Phase Services – The design team will be responsible for providing review of contractor submitted shop drawings, assisting the City in responding to RFIs submitted by the contractor, and performing any necessary NPDES-related inspections if required.

Deliverables:

- All electronic files in original formats
- PDF of all engineering documents, reports, etc.
- Cost estimates at 50%, 90%, and 100% plan submittal

General Information

1. Design work must conform to applicable AASHTO/GDOT guidelines and the Georgia Standard Specifications for the Construction of Transportation Systems 2021 Edition.
2. All proposed crosswalks, sidewalks, and other structures shall be ADA compliant. Design of crosswalks and sidewalk should follow the City's standards and details, including the City's stormwater requirements.
3. Any retaining walls utilized on the project will require a decorative appearance. In the case of cast-in-place retaining walls, the design must incorporate a veneer as selected by the City.
4. Utility coordination will be performed by the selected consultant.

5. Public involvement is not anticipated.
6. Landscaping or lighting may be required.
7. Information regarding land development permitting through the City's Community Development Department (including checklists, stormwater policy, and arborist guidance) can be found here:
<https://www.alpharetta.ga.us/government/departments/community-development/resources>
8. The City of Alpharetta is a LIA with a Memorandum of Agreement.
9. The City will waive all City permitting fees associated with this project.
10. Permits anticipated to be required for this project are the City of Alpharetta Land Disturbance Permit (LDP) and NOI, if one is required. The consultant shall determine if any other permits are required for the construction of this project and shall be responsible for all activities necessary to obtain approved permits.
11. The Consultant shall use the City-developed specification for landscaping. For all other specifications, the Consultant can either utilize the GDOT or any City specification or provide their own.
12. Selected design consultant will be expected to meet monthly with the City to provide progress reports.

Please refer to Appendix A of this document for reference materials.

FOLLOW THIS OUTLINE

How We Want You to Construct Your Response

1. Using Bonfire to Submit Response

- 1.1. This is the link to Bonfire Project Web Page to get our documents and to upload your response: <https://cityofalpharetta.bonfirehub.com/>
- 1.2. We are accepting all responses only online. You must upload completed responses online before the closing date and time found in Project Details of the project web page for this RFQ.
- 1.3. We will not accept responses by mail, fax, or email. We will not accept paper copy responses. We will not accept any responses after the closing time deadline has passed.
- 1.4. You have not completed your response simply by uploading response documents and information. You must successfully upload all the required documents, including filling out any questionnaires or data requests, and then you must click the submit button before the closing time.
- 1.5. You will receive an email confirmation receipt with a unique confirmation number shortly after you complete your response upload. This confirms that you have successfully turned in your response with all required information.
- 1.6. You can update your response at any time until the closing time.
- 1.7. All uploaded items and responses are Sealed and will only be visible by the City after the closing time has passed.
- 1.8. If the file is 'mandatory' or 'required', you won't be able to complete your response until you have met all requirements.
- 1.9. Uploading large documents may take more time, depending on the size of the file(s) and your Internet connection speed.
- 1.10. Pay attention to the type and number of files we have asked you to upload.
- 1.11. The largest upload file size is 1000 MB.
- 1.12. Don't embed any documents within your uploaded files. They won't be accessible or evaluated.
- 1.13. Minimum system requirements: Internet Explorer 11, Microsoft Edge, Google Chrome, or Mozilla Firefox. Java Script must be enabled.

2. Required Response Document Formats

- ❖ Each SOQ must follow these document formats.
 - Failure to follow these formats will reduce our review team's ability to evaluate and will result in a lower proposal score or in complete removal of a proposal from scoring.

- Format your documents using this outline:
 - ☐ formatted to single space lines,
 - ☐ 10 to 12-point font size,
 - ☐ black font color, and
 - ☐ upload proposal documents in PDF format unless otherwise requested.

DOCUMENT 1 Title: **Statement of Qualifications**

- This document must be no more than five (5) pages, exclusive of a cover letter, three (3) single-page project fact sheets, resumes of key personnel (one page per employee) and GDOT pre-qualification forms.
- This document must be in the following order:
 - A. **Cover Letter with Brief Business Profile**, length of time in business, and a summary describing company strong points and why your experience with similar projects will benefit the City.
 - B. **Business information**, including name and home office address. If another office address oversees work of this project, add that address information too.
 - C. **Contact**, one person to be the single point of contact for this response. All communication with the City will be with this person. Supply the following contact information in the response:
 - Name, including business title and preferred personal title (Mr. Ms. etc.)
 - mailing address,
 - telephone number, cell phone number, and
 - e-mail address.
 - D. **Resumes or Statements of Qualifications**. Include resumes or qualifications for Key people that you plan to assign to this project. The information included should be for work history related to this project. At a minimum, include:
 - Employee's name, title, and intended role for this project.
 - Employee's work experience and years performing work like this project.
 - Employee's qualification, education, skills, certifications that may apply.
 - Employee's length of time with your company.
 - Examples of employee's project work that is like our project.
 - E. **Examples of Previous Projects**. Identify three (3) projects with similar scopes successfully completed by consultant team. Each example project does not need to include all elements of this project. However, all project elements should be represented among the example projects. At a minimum include:
 - Contact name, telephone number, and email address
 - Project dates

- Project construction value
 - Brief project scope
 - Identify the involvement of any proposed key personnel
- F. **Project Understanding & Approach.** Briefly discuss your understanding of the project and approach to it.
- G. **Resumes.** Include resumes or qualifications for key people that you plan to assign to this project. The information included should be for work history related to this project. At a minimum, include:
- Employee's name, title, and intended role for this project.
 - Employee's work experience and years performing work like this project.
 - Employee's qualification, education, skills, certifications that may apply.
 - Employee's length of time with your company.
 - Examples of employee's project work that is like our project.
- H. **GDOT Pre-Qualification Forms**

REQUIRED FORMS:

- We have provided a document file with three required forms. You must complete these forms and return to us with every response.
- We prefer all three completed forms returned as one PDF file. However, we won't lower your scoring if you return the forms separately.
- Below are the required forms for all responses:
 - A. **IRS Form W-9**
 - B. **Bidder's Disclosures and Certifications**
 - C. **E-Verify** (Affidavit Verifying Contractor Participation in Federal Work Authorization Program)

- ❖ *E-Verify side note:* Companies return this form to us incorrectly more often than anything else we request in our RFQs.
- ❖ Top mistakes include wrong number or missing information.
- ❖ State of Georgia law requires that we have this completed form before we can review a response.
- ❖ A form with errors doesn't fulfill this requirement.

All the following must be on the E-verify affidavit.

- Federal Work Authorization User Identification Number – this is only five to eight numbers.
 - ⊗ No A, B, Cs.
 - ⊗ It's different from your Tax ID, Employer Identification, or Social Security Number.
 - ⊗ It won't have a combination of letters and numbers.
- Date of Authorization – this is when you first signed up and got the E-verify number.
- Name of Contractor – your company
- Name of Project – Same as RFQ title
- Date, City, and State – when and where this form was signed
- Signature of Authorized Officer or Agent – to be signed
- Printed Name and Title of Authorized Officer or Agent – the person that signed the form.
- Notarized with seal

3. Other Required Information

QUESTIONNAIRE:

We use a questionnaire to gather important information needed for legal requirements, your acknowledgements, our proposal review, or information needed for writing a contract.

Some questions may require your answers about the work we have described in this RFP.

You will fill out the questionnaire provided. There is no other form or document to upload.

Information requests and response types are as follows:

- Authorized signer for contract execution in DocuSign: Supply name, business title, email address [Response Type: text entry].
- Contact for legal notices-needed for contracting: Business name and mailing address, contact name [Response Type: text entry].
- DUNS Number [Response Type: number entry].
- Addenda Acknowledgement, enter the number of addenda received [Response Type: 0, 1, 2, etc].
- Insurance Requirement Acknowledgement [Response Type: Yes, No entry].



Appendix A: Reference Information

1. Location Map: Roswell St at Marietta St
2. Location Map: Academy Street at City Center
3. Location Map: Street Walls along Highway 9



RFQ 22-1007, Design Services: Pedestrian Improvements

Record of Submissions Receipt

Due Date / Time: July 14, 2022; 10:00 AM

Supplier	Date Submitted	Name
Moffatt & Nichol	Jul 14, 2022 8:42 AM EDT	Ron Osterloh
Croy Engineering, LLC	Jul 13, 2022 11:16 AM EDT	Carmen Weaver
Axis Infrastructure, LLC	Jul 14, 2022 8:45 AM EDT	Traci Strom
Columbia Engineering	Jul 13, 2022 6:13 PM EDT	Randy Strunk
Keck & Wood, Inc.	Jul 14, 2022 9:51 AM EDT	Kimberly Roberts



STAFF REPORT

Submitting Department: Public Works

Submitted By: Pam Bush

Sponsored By:

Meeting Date: September 26, 2022

I. AGENDA ITEM TITLE: DESIGN/PROJECT MANAGEMENT SERVICES CHANGE ORDERS FOR WEBB BRIDGE ROAD (NORTH POINT PARKWAY TO CITY LIMITS)
APPROVAL OF CHANGE ORDER #3 TO PURCHASE ORDER 19000583 FOR POND & COMPANY AND CHANGE ORDER #2 TO PURCHASE ORDER 19000584 FOR ATKINS.

II. RECOMMENDATION:

Approve the following change orders in accordance with the City's Procurement Policy: (a) Change Order #3 to Purchase Order 19000583 for Pond & Company in the amount of \$25,710.00 for design revisions to the Webb Bridge Road (Greenway to Webb Bridge Way); (b) Change Order #2 to Purchase Order 19000584 for Atkins in the amount of \$36,700.00 for additional project management services; and authorize the Mayor to execute all necessary documents.

III. BUDGET IMPLICATIONS:

BUDGETED ITEM: YES

FISCAL IMPACT: YES

INCLUDED IN CURRENT FY CPTL BUDGET: YES INCLUDED IN CURRENT FY OPRT. BUDGET: NO

TOTAL PROJECT COST:

APPROPRIATIONS:

ACCOUNT TITLE/NUMBER	DOLLAR AMOUNT
Pond - WBR PH2 (TSPLOST 2; Roundabout-Park) 33541100-541410-C2229	\$25,710
Atkins - WBR PH2 (TSPLOST 2; Roundabout-Park) 33541100-541410-C2229	\$36,700

EXTERNAL FUNDING SOURCES:

ACCOUNT TITLE/NUMBER	DOLLAR AMOUNT
NA	\$0.00
NA	\$0.00

IV. REPORT IN BRIEF:

The Webb Bridge Road improvement Project consists of providing a 10.5-foot travel lane, a 4-foot bike lane, a 0.5-foot header curb, a 6-foot planting strip, and a 10-foot sidewalk along both sides of Webb Bridge Road. Left turn lanes and median landscape islands will be provided where appropriate. Pedestrian lighting and street trees will be provided in the planting strip. A roundabout will be constructed at the intersection of Webb Bridge Road and Webb Bridge Way, replacing the existing traffic signal.

The Webb Bridge Road project has multiple phases including:

Phase 1: Northern section of Webb Bridge Road from the Big Creek Greenway tunnel to Westwind Lane that has recently been constructed.

Phase 2A: Construction of a roundabout at the intersection of Webb Bridge Road and Webb Bridge Way and improvements along the north side of Webb Bridge Road from the future roundabout to Webb Bridge Park. Currently, there is a traffic light at the intersection of Webb Bridge Road and Webb Bridge Way that will be replaced with a roundabout. Design work for this phase has been completed and will be out to bid for construction in September 2022. Right-of-way acquisition for this phase is nearly complete. It is anticipated to award construction of this phase to a contractor around December 2022.

Phase 2B: Construction of the remainder of the project from the Big Creek Greenway tunnel to Webb Bridge

Way. This phase is currently under design and right-of-way acquisition of 47 parcels. Based on the number of parcels to acquire right of way and or easements, staff believe it will be another year before this phase will be bid out.

Phase 3: Construction of the section from North Point Parkway to the Big Creek Greenway tunnel, including replacing the bridge across Big Creek. Design work for this phase has been completed and will be out to bid for construction in September 2022. ROW acquisition for this phase is nearly complete. It is anticipated to award construction of this phase to a contractor around December 2022.

Design Work by Pond & Company:

On May 6, 2019, City Council approved Pond & Company's proposal for the design of improvements to Webb Bridge Road from the Big Creek Greenway to Webb Bridge Way for an amount of \$499,717.50 (Purchase Order 19000583).

On November 11, 2019, City Council approved Change Order #1 that adjusted the scope of the project to include continuation of wider sidewalks from the Webb Bridge Way intersection to the entrance of Webb Bridge Park and to the City Limits near Kimball Bridge Road. Change Order #1 increased the design cost by \$155,942.96 from \$499,717.50 to \$655,660.46.

On October 19, 2020, City Council approved Change Order #2 that adjusted the scope of the project to widen the planting area from 4' to 6' and the sidewalk from 8' to 10' along both sides of Webb Bridge Road, increasing the design cost by \$123,415.00 from \$655,660.46 to \$779,075.46.

During the right of way acquisition phase, residents have recently requested changes to the plans; and to accommodate residents' requests, re-designing of sidewalks, planting areas, and geometry of Webb Bridge Road is necessary. Modifying the designs to accommodate various requests from the citizens will save dollars in right-of-way/easement acquisition as well as in construction costs. The trade-off is that the corridor will not be 100% consistent, but this is common in retrofitting corridors in established communities with limited right-of-way availability. To this end, staff is recommending approval of Change Order #3 to Purchase Order 19000583 for Pond & Company that will increase the design cost by \$25,710.00 (from \$779,075.46 to \$804,785.46). PW staff has reviewed the hours and they appear reasonable for the assignment and the rates are in accordance with the original PO.

Project Management by Atkins North America, Inc:

On May 6, 2019, City Council approved Atkins proposal for project management services associated with Pond & Company's design of the Webb Bridge Road and Academy Street project for a total amount of \$109,000.00.

When Pond proposed their initial change order in November 2019, Atkins did not submit a change order request and believed they could absorb the cost of the continued plan review and project management. Change Order #1 from Atkins was submitted and approved on 10/19/2020 when Pond submitted their second change order. Atkins first change order increased the Webb Bridge Road project management cost by \$25,000.00 from \$109,000.00 to \$134,000.00. Between October 2020 and now, the corridor project went through some challenges regarding QAQC (quality assurance and quality control) issues with the design team. Addressing these issues required Atkins to spend more time than originally estimated and absorbed dollars allocated for the entire corridor.

Along with Pond's third change order, which is to re-design the sidewalk and plating strip at multiple segments in Phase 2B (from the Big Creek Greenway tunnel to Webb Bridge Way), Atkins is requesting additional funds for continued project management associated with the proposed design revisions and bid assistance for the entire corridor. Atkins' experience in bridge construction is required to answer questions during the bid phase from the contractors regarding phase 3 (North Point Parkway to the Big Creek Greenway tunnel). Change Order #2 from Atkins will increase the Webb Bridge Road project management cost by \$36,700.00 from \$134,000.00 to \$170,700.00. PW staff has reviewed the hours and they appear reasonable for the assignment and the rates are in accordance with the original PO.

V. ALTERNATIVES:

None.

VI. ATTACHMENTS:



3500 Parkway Lane, Suite 500
Peachtree Corners, Georgia 30092

T: 678.336.7740 | F: 678.336.7744
www.pondco.com

August 15, 2022

Mr. Peter Sewczwicz, PE
Director of Public Works
City of Alpharetta
1790 Hembree Road
Alpharetta, GA 30009

Re: **Webb Bridge Road Bike/Ped/Operational Improvements from Big Creek Greenway to Webb Bridge Way
Additional Services Fee Proposal – Change Order #3**

PROFESSIONAL SERVICES:

At the request of the City, this additional services fee proposal is for pending and potential ROW revisions that will necessitate design and plan changes. One pending revision includes changing the typical section in front of parcels 36 and 38 to eliminate the landscaping strip and reduce the sidewalk to 8' in width. We will update the model to develop new limits of construction. We will add notes and labels as needed to make the contractor aware that the existing fence and landscaping on these parcels are not to be disturbed. To avoid impacts to the existing fence and landscaping, we will need a gravity wall on the eastern edge of parcel 38. Potential anticipated ROW revisions include Parcel 19 where a portion of the entry fence for this new development was constructed within the proposed ROW, Parcel 40 where the property owner recently constructed a new privacy fence and landscaping within the proposed ROW, and Parcels 48 and 50 where the new subdivision signs were constructed inside the existing ROW and proposed easements. It is assumed these ROW revisions will result in similar changes to the typical section as proposed along Parcels 36 and 38.

Changes to the typical section will impact other design elements and associated sheets, such as landscaping, lighting, and erosion control. All impacted plan sheets will be updated with the new typical section in these areas.

We are proposing that this SA will add fee to Phase 4: Final Bid Plans for both the construction plan and ROW plan revisions needed.

Scope of Work

Phase 4 – Change Order 3

- **Pending ROW revision:** Revise Typical Section along Webb Bridge Road in front of Parcels 36 and 38 to eliminate the planting strip and reduce the sidewalk to 8'. A small gravity wall will be needed on the eastern edge of Parcel 38. This change will in-turn impact the current roadway plans, landscaping, lighting, erosion control, quantities, and ROW plans.
- **Potential ROW Revisions:** Revise Typical Section along Webb Bridge Road in front of impacted Parcels 36 and 38 to eliminate adverse impact to the owners' areas of concern (i.e. fence, landscaping, signage, etc. A small gravity wall may be needed at the back of sidewalk for at least one parcel. These change will in-turn impact the current roadway plans, landscaping, lighting, erosion control, quantities, and ROW plans.

The expected specific tasks involved in the development of the above elements are contained in the attached Schedule of Fees.

ASSUMPTIONS

Services or tasks not specifically outlined above or in the attached Schedule of Fees are excluded. This scope and fee assume no additional staging design and plans are needed for the revised typical section. No additional SUE services, environmental services, traffic services, or construction administration are part of this current scope.

PROFESSIONAL FEES:

Pond proposes to accomplish this work for a proposed total fee of \$25,710.00. We understand that to utilize fees from this SA, we must receive a written notice to proceed (emails will be sufficient) that contains the limiting amount per parcel/task.

If you need any additional information, please feel free to contact me at (470)387-8949.

Sincerely,

POND & COMPANY

James McNabb, P.E.
Sr. Vice President

Cc: Arwin Lopez, P.E.; Tabatha Carlton, P.E.

Attachments: Schedule of Fees

City of Alpharetta

Webb Bridge Rd from Big Creek Greenway to Webb Bridge Way Bike/Ped and Operational Improvements Project Length 1.85 miles

SUMMARY BY Segment

COST AMOUNT OF CONTRACT CHANGE ORDER PROPOSAL

8/15/2022

	PHASE AMOUNTS
Phase 4 - SA #3 Revise Plan sheets and ROW plans due to ROW Negotiations	\$ 25,710.00
TOTAL DESIGN COST FOR ALL SEGMENTS	\$ 25,710.00

City of Alpharetta

Phase 4 summary

PROJECT: Webb Bridge Rd from Big Creek Greenway to Webb Bridge Way

Phase 4 - SA #3 Revise Plan sheets and ROW plans due to ROW Negotiations

PERSONNEL	EST. HOURS	RATE/HR.	COST \$	TOTALS
PRINCIPAL	8	\$ 200.00	\$ 1,600.00	
PROGRAM MANAGER	13	\$ 180.00	\$ 2,340.00	
PROJECT MANAGER	19	\$ 160.00	\$ 3,040.00	
SENIOR ENGINEER	44	\$ 130.00	\$ 5,720.00	
ENGINEER	78	\$ 100.00	\$ 7,800.00	
SENIOR LANDSCAPE AR	4	\$ 110.00	\$ 440.00	
LANDSCAPE ARCHITECT	13	\$ 90.00	\$ 1,170.00	
TECHNICIAN/DRAFTER	45	\$ 80.00	\$ 3,600.00	
ADMINISTRATIVE ASSIST	0	\$ 60.00	\$ -	
GIS ANALYST	0	\$ 85.00	\$ -	
SENIOR REGULATORY S	0	\$ 155.00	\$ -	
PROJECT SCIENTIST 1	0	\$ 110.00	\$ -	
SCIENTIST 2	0	\$ 95.00	\$ -	
SCIENTIST 1	0	\$ 75.00	\$ -	
TOTAL DIRECT LABOR		224 Manhours	\$	25,710.00
DIRECT COSTS (SPECIFY):				
ITEM	UNIT COST	QUANTITY	TOTALS	
Mileage (30 miles roundtrip to proj. site)	\$ 0.55	0	\$ -	
REPRODUCTION	\$ 150.00		\$ -	
MAIL & DELIVERY	\$ 50.00		\$ -	
TRAVEL	\$ -		\$ -	
Direct Cost Total				\$ -
SUBCONSULTANTS (LIST):				
SUB CONSULTANT			TOTALS	
			\$ -	
Subconsultant Sub Total				\$ -
COST AMOUNT FOR PHASE				\$ 25,710.00

City of Alpharetta
Phase 4 detail

PROJECT: Webb Bridge Rd from Big Creek Greenway to Webb Bridge Way
Phase 4 - SA #3 Revise Plan sheets and ROW plans due to ROW Negotiations

TASKS	Assumptions: Current Phase to last 2 months	No. of SHT	PRINCIPAL	PROGRAM MANAGER	PROJECT MANAGER	SENIOR ENGINEER	ENGINEER	SENIOR LANDSCAPE ARCHITECT	LANDSCAPE ARCHITECT	TECHNICIAN/ DRAFTER	TOTAL	% OF TOTAL
Non-Drawing Tasks												
Deliverables												
Revise Typical Section in front of Parcels 36 and 38												
Revise Typical sections		1				1	1			1	3	1.3%
Modify Planview		2				1	1			1	3	1.3%
Modify InRoads Model						1	2				3	1.3%
Create Wall Envelope		1				1	3				4	1.8%
Modify Cross section		2				1	2				3	1.3%
Modify Drainage		1					1			1	2	0.9%
Modify Lighting		2	1			1	4			1	7	3.1%
Modify Landscape		2	1					1	4	1	7	3.1%
Modify Erosion Control Plans		8				1	4			2	7	3.1%
Modify Base files on all other series and correct overwrites		6				1	1			4	6	2.7%
Update Quantities and Eng. Estimate		4				2	3			1	6	2.7%
QA/QC and PM Coordination			1	2	4	2					9	4.0%
Utility Coordination				1	2						3	1.3%
Revise ROW Plans		2	1	1	1	1	2				6	2.7%
Other potential ROW revisions (See list below)												
Revise Typical sections		3				3	3			3	9	4.0%
Modify Planview		4				3	3			3	9	4.0%
Modify InRoads Model						3	6				9	4.0%
Create Wall Envelope		1				1	3				4	1.8%
Modify Cross section		6				3	6				9	4.0%
Modify Drainage		3					3			3	6	2.7%
Modify Lighting		4	1			3	9			3	16	7.1%
Modify Landscape		4	1					3	9	3	16	7.1%
Modify Erosion Control Plans		12				3	9			6	18	8.0%
Modify Base files on all other series and correct overwrites		18				3	3			9	15	6.7%
Update Quantities and Eng. Estimate		12				3	6			3	12	5.4%
QA/QC and PM Coordination			1	3	6	3					13	5.8%
Utility Coordination				3	3						6	2.7%
Revise ROW Plans		4	1	3	3	3	3				13	5.8%
Other potential ROW revisions list												
Parcel 40 - Avoid new fence and landscaping												
Parcel 48 & 50 - New subdivision signs constructed in existing and proposed ROW												
Parcel 19 - Existing entry way fence was constructed in ROW												
TOTALS		102	8	13	19	44	78	4	13	45	224	100.0%



Webb Bridge Road Corridor - North Point Parkway to City limits
September 8, 2022

Task ID	Description	Directs/ Expenses	PIC Hours	PM Hours	Dep PM	CM Hours	Labor Price	Total Price (Labor + Directs)
	Rate	N/A	\$ 341.10	\$ 242.24	\$ 167.97	\$ 265.44		
01	Final Review of plans	\$30.00	1	20	8	12	\$ 9,714.83	\$ 9,744.83
02	Review of ROW plans and revisions	\$30.00	0	16	16	14	\$ 10,279.40	\$ 10,309.40
03	Assistance with bid package	\$29.01	0	16	0	48	\$ 16,616.77	\$ 16,645.78
								\$ 36,700.00

PIC Principal in Charge (Brian Bolick)
PM Project Manager (Nikki Parris)
CM Project Manager (Obie Brannon)
Dep PM Deputy PM (Nicole Neeley)



STAFF REPORT

Submitting Department: Information Technology

Submitted By: Randy Bundy

Sponsored By:

Meeting Date: September 26, 2022

I. AGENDA ITEM TITLE: MS-ISAC SECURITY SOFTWARE

APPROVAL OF THE PURCHASE OF the CIS Albert MD Appliance Primary Sensor System FROM THE CENTER FOR INTERNET SECURITY, INC.

II. RECOMMENDATION:

Please authorize the purchase of the CIS Albert MD Appliance Primary Sensor System from the Center for Internet Security, Inc. (sole source provider) for an amount totaling \$34,200 and authorize the Mayor to execute all necessary documents.

III. BUDGET IMPLICATIONS:

BUDGETED ITEM: NO

FISCAL IMPACT: YES

INCLUDED IN CURRENT FY CPTL BUDGET: NO

INCLUDED IN CURRENT FY OPRT. BUDGET: NO

TOTAL PROJECT COST: \$34,200.00

APPROPRIATIONS:

<u>ACCOUNT TITLE/NUMBER</u>	<u>DOLLAR AMOUNT</u>
Across Multiple Departments - Professional Services	\$34,200.00

EXTERNAL FUNDING SOURCES:

<u>ACCOUNT TITLE/NUMBER</u>	<u>DOLLAR AMOUNT</u>
N/A	\$0.00

IV. REPORT IN BRIEF:

The City of Alpharetta is a member of the Multi-State – Information Sharing and Analysis Center (MS-ISAC), which is a division of the Center for Internet Security (CIS), which is funded by DHS. The MS-ISAC's role is to provide cybersecurity information and tools to state, local, tribal, and territory governments (SLTT). As such, CIS is the sole source provider of these systems.

The City receives a great deal of information from them and participates in the nationwide meetings and cybersecurity training at no charge to the City. CIS offers an Intrusion Detection System (IDS) called Albert Monitoring at a cost to MS-ISAC and EL-ISAC (election entity) members. This IDS requires a hardware component to collect network traffic that is entering and leaving our network through our internet circuits. The collected data is sent to the CIS Security Operations Center (SOC) where it is analyzed against known bad traffic. Once traffic is flagged as potentially bad, a professional in their SOC reviews further and contacts us if they believe an incident is occurring.

Albert Monitoring is becoming a standard in state and local government operations. We know most state governments, including Georgia, have implemented it along with hundreds of local governments. The analysis being done is specific to governments and is fed by all the data collected, the federal SOC (CISA, NSA, DoD, DHS), and private organizations. In addition to the monitoring and analysis, the offering also comes with incident response capabilities. The CIS Cyber Incident Response Team (CIRT) will assist in any remediation, mitigation, and forensic work to be done in the event of an incident. This has become more important recently as the State now requires notification of an incident or event.

There is a one-time implementation cost of \$1,800. The remainder of \$32,400.00 will be the annual operating cost. This request was not funded in the current budget. However, given the increasing threats, the rising cost of remediation from attacks, the high value of the offering, and the relatively low cost of the offering, IT recommends we should purchase and implement Albert Monitoring from the Center for Internet Security (sole

source provider). Funding will be reprioritized to cover this needed service and the necessary funding requested as part of the mid-year 2023 budget process.

V. ALTERNATIVES:

NONE

VI. ATTACHMENTS:

CIS - Single Source Justification Language, CIRT Roles and Responsibilities,
National_Cyber_Incident_Response_Plan, ITSS Plan, Albert Monitoring Datasheet, City of
Alpharetta_Order_2MDTurnkey_Aug26_2022

The Center for Internet Security (CIS) is a nonprofit organization focused on enhancing the cyber security readiness and response of public and private sector entities. CIS operates the Multi-State Information Sharing and Analysis Center (MS-ISAC), which is designated by the U.S. Department of Homeland Security as the key resource for cyber threat prevention, protection, response and recovery for the nation's state, local, tribal, and territorial (SLTT) government entities. Through its state-of-the-art 24/7/365 cyber security operations center, CIS serves as a central resource for situational awareness and incident response for SLTT governments, and offers a number of strategic cyber security services to assist in detecting, protecting, responding to and recovering from cyber threats.

The CIS Netflow/Intrusion Detection System Monitoring and Analysis Service, known as Albert, provides our partners with a near real-time automated process that identifies and alerts on traditional and advanced threats on a network, facilitating rapid response to threats and attacks. The Albert sensor(s) provide traditional Intrusion Detection System (IDS) monitoring, along with netflow and passive DNS collection and analysis. Through its 24/7/365 Security Operations Center (SOC), CIS manages the sensor(s) to identify malicious activity, and, in accordance with escalation procedures prescribed by the partner, provides notification of malicious activity. The use of open source software allows CIS to provide enhanced monitoring capabilities in a more affordable, cost-effective way than a typical commercial IDS/IPS solution.

Why is the CIS Albert Service Unique?

- Government-specific focus and tailored to SLTT government's cyber security needs.
- Correlation of data from multiple public and private partners
 - Historical log analysis performed on all logs collected for specific threats reported by partners and/or trusted third parties.
 - When a major new threat is identified, CIS will search logs for prior activity. (Traditional monitoring services only alert going forward, from the date a signature is in place. There is no "look behind" to assess what activity may have already occurred.)
- Statistical analysis of traffic patterns to areas of the world known for being major cyber threats. If abnormal traffic patterns are detected, analysts review the traffic to determine the cause, looking for malicious traffic that is not detected by signatures.
- Signatures from forensic analysis of hundreds of SLTT cyber incidents are added to the signature repository.
- Integration of research on threats specific to SLTTs, including nation-state attacks.
- CIS staff permanently deployed at the National Cybersecurity and Communications Integration Center (NCCIC) in Washington, D.C, thus facilitating valuable real-time information sharing with federal partners and critical infrastructure sectors.
- Experienced cyber security analysts who review each cyber security event, which results in minimizing the number of false-positive notifications, allowing the first responder to focus on actionable events.
- Availability of an Incident Response Team for forensic and malware analysis which is of no cost to SLTT government entities.
- 24/7/365 technical, research, and remediation support for cyber security incidents.



CIRT Roles and Responsibilities

Incident Response and Computer Forensic Examinations



The MS-ISAC provides cyber incident response services free of cost to State, Local, Tribal, and Territorial (SLTT) organizations. These services are provided by our Cyber Incident Response Team (CIRT), a team of highly knowledgeable and skilled analysts trained in digital forensics and incident response. Services include:

- Emergency conference calls
- Log analysis
- Ongoing communication throughout the incident
- Mitigation recommendations (Attended Remediation)
- Computer forensic analysis of forensic images to determine root cause analysis as needed in support of an ongoing incident response case
- At the close of the incident, written communication will be provided that summarizes the incident.
- In every incident, CIRT exerts a concerted effort to provide a personal level of service to SLTT organizations, seeking to engage with customers based on their organizational needs and circumstances.



NATIONAL CYBER INCIDENT RESPONSE PLAN

December 2016



**Homeland
Security**

This page intentionally left blank.

Table of Contents

EXECUTIVE SUMMARY	4
INTRODUCTION.....	6
SCOPE	6
GUIDING PRINCIPLES.....	7
RELATIONSHIP TO NATIONAL PREPAREDNESS SYSTEM.....	8
ROLES AND RESPONSIBILITIES.....	10
CONCURRENT LINES OF EFFORT	11
THREAT RESPONSE	12
Private Sector.....	12
State, Local, Tribal, and Territorial Governments	13
Federal Government	13
ASSET RESPONSE.....	14
Private Sector.....	14
State, Local, Tribal, and Territorial Government	16
Federal Government	17
INTELLIGENCE SUPPORT	19
State, Local, Tribal, and Territorial Government.....	19
Federal Government	20
AFFECTED ENTITY'S RESPONSE	21
Cyber Incidents Involving Personally Identifiable Information	21
CORE CAPABILITIES	21
Access Control and Identity Verification	22
Cybersecurity.....	22
Forensics and Attribution.....	22
Infrastructure Systems.....	23
Intelligence and Information Sharing.....	23
Interdiction and Disruption.....	23
Logistics and Supply Chain Management.....	24
Operational Communications	24
Operational Coordination	24
Planning	24
Public Information and Warning.....	25
Screening, Search, and Detection.....	25
Situational Assessment.....	25
Threats and Hazards Identification.....	25
COORDINATING STRUCTURES AND INTEGRATION.....	26
COORDINATING STRUCTURES.....	26
Private Sector.....	26
State, Local, Tribal, and Territorial Governments	27
Federal Government	28
International	29
OPERATIONAL COORDINATION DURING A SIGNIFICANT CYBER INCIDENT	29
Determination of Incident Severity.....	29
Enhanced Coordination Procedures.....	31
Cyber UCG	31
Information Sharing During Cyber Incident Response.....	34

CONCLUSION	34
ANNEX A: AUTHORITIES AND STATUTES.....	36
ANNEX B: CYBER INCIDENT SEVERITY SCHEMA.....	38
ANNEX C: CYBER INCIDENT SEVERITY SCHEMA/ NATIONAL RESPONSE COORDINATION CENTER ACTIVATION CROSSWALK.....	39
ANNEX D: REPORTING CYBER INCIDENTS TO THE FEDERAL GOVERNMENT	40
ANNEX E: ROLES OF FEDERAL CYBERSECURITY CENTERS	43
ANNEX F: CORE CAPABILITIES AND CRITICAL TASKS.....	45
ANNEX G: DEVELOPING AN INTERNAL CYBER INCIDENT RESPONSE PLAN	53
ANNEX H: CORE CAPABILITY/NIST CYBERSECURITY FRAMEWORK/PPD-41 CROSSWALK.....	54
ANNEX I: ADDITIONAL RESOURCES	59
ANNEX J: ACRONYM LIST	60

Executive Summary

Networked technologies touch every corner of the globe and every facet of human life. They have driven innovation, nurtured freedoms, and spurred economic prosperity. Even so, the very technologies that enable these benefits offer new opportunities for malicious and unwanted cyber activities. The risks associated with the Nation's dependence on these networked technologies led to the development of Presidential Policy Directive 41 (PPD-41): *United States Cyber Incident Coordination*, which sets forth principles governing the Federal Government's response to any cyber incident, whether involving government or private sector entities.

PPD-41 recognizes that the frequency of cyber incidents is increasing, and this trend is unlikely to be reversed anytime soon. The most significant of these incidents, those likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people, necessitate deliberative planning, coordination, and exercising of response activities, in order to minimize the threat and consequences to the Nation, infrastructure, and way of life.

The National Cyber Incident Response Plan (NCIRP or Plan) was developed according to the direction of PPD-41 and leveraging doctrine from the National Preparedness System to articulate the roles and responsibilities, capabilities, and coordinating structures that support how the Nation responds to and recovers from significant cyber incidents posing risks to critical infrastructure. The NCIRP is not a tactical or operational plan; rather, it serves as the primary strategic framework for stakeholders to understand how federal departments and agencies and other national-level partners provide resources to support response operations. Authored in close coordination with government and private sector partners, the NCIRP expounds upon the concurrent lines of effort, defined by PPD-41, for how the Federal Government will organize its activities to manage the effects of significant cyber incidents. The concurrent lines of effort are threat response, asset response, intelligence support, and the affected entity, which undertakes efforts to manage the effects of the incident on its operations, customers, and workforce. The activities and lead federal agencies for each line of effort within the Cyber Unified Coordination Group are described below.

- The Department of Justice is the lead agency for threat response during a significant cyber incident, acting through the Federal Bureau of Investigations and National Cyber Investigative Joint Task Force. Threat response activities include conducting appropriate law enforcement and national security investigative activity at the affected entity's site; collecting evidence and gathering intelligence; providing attribution; linking related incidents; identifying additional affected entities; identifying threat pursuit and disruption opportunities; developing and executing courses of action to mitigate the immediate threat; and facilitating information sharing and operational coordination with asset response.
- The Department of Homeland Security is the lead agency for asset response during a significant cyber incident, acting through the National Cybersecurity and Communications Integration Center. Asset response activities include furnishing technical assistance to affected entities to protect their assets, mitigate vulnerabilities, and reduce impacts of cyber incidents; identifying other entities that may be at risk and assessing their risk to the same or similar vulnerabilities; assessing potential risks to the sector or region, including potential cascading effects, and developing courses of action to mitigate these risks; facilitating information sharing and

operational coordination with threat response; and providing guidance on how best to utilize federal resources and capabilities in a timely, effective manner to speed recovery.

- Threat and asset responders will share some responsibilities and activities, which may include communicating with affected entities to understand the nature of the cyber incident; providing guidance to affected entities on available federal resources and capabilities; promptly disseminating through appropriate channels intelligence and information learned in the course of the response; and facilitating information sharing and operational coordination with other Federal Government entities.
- The Office of the Director of National Intelligence is the lead coordinator for intelligence support during a significant cyber incident, acting through the Cyber Threat Intelligence Integration Center. Intelligence support and related activities include providing support to federal asset and threat agencies and facilitate the building of situational threat awareness and sharing of related intelligence; the integrated analysis of threat trends and events; the identification of knowledge gaps; and the ability to degrade or mitigate adversary threat capabilities.
- An affected federal agency shall engage in a variety of efforts to manage the impact of a cyber incident, which may include maintaining business or operational continuity; addressing adverse financial impacts; protecting privacy; managing liability risks; complying with legal and regulatory requirements (including disclosure and notification); engaging in communications with employees or other affected individuals; and dealing with external affairs (e.g., media and congressional inquiries). The affected federal agency will have primary responsibility for this line of effort.
- When a cyber incident affects a private entity, the Federal Government typically will not play a role in this line of effort, but it will remain cognizant of the affected entity's response activities, consistent with the principles above and in coordination with the affected entity. The relevant sector-specific agency will generally coordinate the Federal Government's efforts to understand the potential business or operational impact of a cyber incident on private sector critical infrastructure.

The NCIRP builds upon these lines of effort to illustrate a national commitment to strengthening the security and resilience of networked technologies and infrastructure. This Plan outlines the structure and content from which stakeholders can leverage to inform their development of agency-, sector-, and organization-specific operational response plans. Correspondingly, this Plan should be understood to be a living document, to be updated as needed to incorporate lessons-learned, to reflect opportunities and challenges that arise as technology evolves, and to ensure the Plan adequately addresses a changing threat/hazard environment.

Introduction

The *National Cybersecurity Protection Act of 2014* (NCPA)¹ consequently codified in the *Homeland Security Act*², mandates that the Department of Homeland Security (DHS), in coordination with appropriate entities and individuals, develop, regularly update, maintain, and exercise adaptable cyber incident response plans to address cybersecurity risks to critical infrastructure. Presidential Policy Directive (PPD)-41: *U.S. Cyber Incident Coordination* and the associated Annex,³ set forth principles governing the Federal Government's response to any cyber incident, provide an architecture for coordinating the response to significant cyber incidents, and required DHS to develop a National Cyber Incident Response Plan (NCIRP or Plan) to address cybersecurity risks to critical infrastructure. The NCIRP is part of the broader National Preparedness System and establishes the strategic framework and doctrine for a whole-of-Nation⁴ approach to mitigating, responding to, and recovering from a cyber incident. This approach includes and strongly relies on public and private partnerships to address major cybersecurity risks to critical infrastructure.

- Response Plan Purpose and Organization – The NCIRP provides guidance to enable a coordinated whole-of-Nation approach to response activities and coordination with stakeholders during a significant cyber incident impacting critical infrastructure. The NCIRP sets common doctrine and a strategic framework for national, sector, and individual organization cyber operational plans.
- Intended Audience – The intended audience for the NCIRP is U.S. organizations. However, it may also enhance our international partners' understanding of the U.S. cyber incident coordination. This whole-of-Nation concept focuses efforts and enables the full range of stakeholders—the private and nonprofit sectors (including private and public owners and operators of critical infrastructure), state, local, tribal, territorial (SLTT) governments, and the Federal Government—to participate and be full partners in incident response activities. Government resources alone cannot meet all the needs of those affected by significant cyber incidents. All elements of the community must be activated, engaged, and integrated to respond to a significant cyber incident.

Scope

Cyber incident response is an important component of information and communications technology (ICT) and operational technology programs and systems. Performing incident response effectively is a complex undertaking and requires substantial planning and resources to establish a successful incident response capability.

The NCIRP is the strategic framework for operational coordination among federal and SLTT governments, the private sector, and international partners. Developed according to the guiding principles outlined in PPD-41 and leveraging doctrine from the National Preparedness System and

¹ The National Cybersecurity Protection Act of 2014. Public Law 113-282. December 18, 2014)).
<https://www.congress.gov/113/plaws/publ282/PLAW-113publ282.pdf>.

² 6 U.S.C § 149

³ PPD-41: *U.S. Cyber Incident Coordination*. <https://www.whitehouse.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident>; Annex for Presidential Policy Directive-41--United States Cyber Incident Coordination, <https://www.whitehouse.gov/the-press-office/2016/07/26/annex-presidential-policy-directive-united-states-cyber-incident>.

⁴ The whole-of-Nation approach also encompasses a wide range of new and existing public and private partnerships to leverage as a platform in working towards managing cybersecurity threats and hazards to critical infrastructure.

the National Incident Management System (NIMS),⁵ the NCIRP sets the strategic framework for how the Nation plans, prepares for, and responds to cyber incidents by establishing an architecture for coordinating the broader community response during a significant cyber incident in accordance with U.S. law and policy. A list of authorities is found in Annex A: Authorities and Statutes. The NCIRP is also designed to integrate and interface with industry standards and best practices for cybersecurity risk management, as developed by the National Institute of Standards and Technology's (NIST) Framework for Improving Critical Infrastructure Cybersecurity.⁶

The NCIRP is not a tactical or operational plan for responding to cyber incidents. However, it should serve as the primary strategic framework for stakeholders when developing agency-, sector-, and organization-specific operational plans. This Plan will help those affected by cyber incidents understand how federal departments and agencies and other national-level partners provide resources to support SLTT and private sector response operations. It should also serve as the basis for national cyber operational playbooks and individual critical infrastructure sector operational coordination plans, as well as be referenced by individual entities in their own plan development. In all cases, incident response activities will be conducted in accordance with applicable law and policy.

Guiding Principles

The NCIRP is based on several guiding principles outlined in PPD-41 for the response to any cyber incident, whether involving government or private sector entities. These principles include:

- Shared Responsibility. Individuals, the private sector, and government agencies have a shared vital interest and complementary roles and responsibilities in protecting the Nation from malicious cyber activity and managing cyber incidents and their consequences.
- Risk-Based Response. The Federal Government will determine its response actions and the resources it brings to bear based on an assessment of the risks posed to an entity, our national security, foreign relations, the broader economy, public confidence, privacy and civil liberties, or the public health and safety of the American people. Critical infrastructure entities also conduct risk-based response calculations during cyber incidents to ensure the most effective and efficient utilization of resources and capabilities.
- Respecting Affected Entities. To the extent permitted under law, Federal Government responders will safeguard details of the incident, as well as privacy, civil liberties, and sensitive private sector information, and generally will defer to affected entities in notifying other affected private sector entities and the public. In the event of a significant cyber incident where the Federal Government interest is served by issuing a public statement concerning an incident, federal responders will coordinate their approach with the affected entities to the extent possible.
- Unity of Governmental Effort. Various government entities possess different roles, responsibilities, authorities, and capabilities that can all be brought to bear on cyber incidents. These entities must coordinate efforts to achieve optimal results. The first federal agency to become aware of a cyber incident will rapidly notify other relevant federal agencies to facilitate a unified federal response and ensure that the right combination of agencies responds to a particular incident. When responding to a cyber incident in the private sector, unity of effort synchronizes the overall federal response, which prevents gaps in service and duplicative efforts. SLTT governments also have responsibilities, authorities, capabilities, and resources that can be

⁵ NIMS. <http://www.fema.gov/national-incident-management-system>.

⁶ Framework for Improving Critical Infrastructure Cybersecurity, version 1.0. National Institute of Standards and Technology, February 12, 2014. <https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf>.

used to respond to a cyber incident; therefore, the Federal Government must be prepared to partner with SLTT governments in its cyber incident response efforts. The transnational nature of the Internet and communications infrastructure requires the United States to coordinate with international partners, as appropriate, in managing cyber incidents.

- **Enabling Restoration and Recovery.** Federal response activities will be conducted in a manner to facilitate restoration and recovery of an entity that has experienced a cyber incident, balancing investigative and national security requirements, public health and safety, and the need to return to normal operations as quickly as possible.

While steady-state activities and the development of a common operational picture are key components of the NCIRP, the Plan focuses on building the mechanisms needed to respond to a significant cyber incident. Table 1 below describes the difference between a “cyber incident” and a “significant cyber incident” as outlined in PPD-41. The Federal Government uses the Cyber Incident Severity Schema (detailed in Annex B: Cyber Incident Severity Schema) to describe the incident level, the process to determine the severity of an incident, and the threshold for designating a significant cyber incident affecting the United States or its interest abroad. The United States Computer Emergency Readiness Team (US-CERT) website also provides a list of types of common ways cyber incidents can occur and exploit information and assets.⁷

Table 1: Cyber Incident Definitions from PPD-41

Incident	Definition
Cyber Incident	An event occurring on or conducted through a computer network that actually or imminently jeopardizes the confidentiality, integrity, or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon.
Significant Cyber Incident	A cyber incident that is (or group of related cyber incidents that together are) likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people.

Relationship to National Preparedness System

While the NCIRP focuses on cyber incident response efforts, the National Preparedness System outlines a broader architecture that establishes how the broader community⁸ prevents, protects against, mitigates, responds to, and recovers from all threats and hazards. Specifically, the National

⁷ <https://www.us-cert.gov/incident-notification-guidelines#attack-vectors-taxonomy>

⁸ The Response Federal Interagency Operational Plan, Second Edition, August 2016, describes the whole community and includes all individuals and household members, specifically inclusive of people with disabilities, children, older Americans, people with different levels of language English proficiency, communities, the private and nonprofit sectors, faith-based organizations, and local, state, tribal, territorial, insular area, and the Federal Government—and the Nation as a whole. https://www.fema.gov/media-library-data/1471452095112-507e23ad4d85449ff131c2b025743101/Response_FIOP_2nd.pdf

Response Framework (NRF)⁹ sets the doctrine and provides guidance for how the Nation builds, sustains, and delivers the response core capabilities identified in the National Preparedness Goal.¹⁰ To further connect the NCIRP with the NRF, the Homeland Security Act¹¹ states the Secretary of DHS, in coordination with the heads of other appropriate federal departments and agencies, and in accordance with the NCIRP under that Act, shall regularly update, maintain, and exercise the Cyber Incident Annex to the NRF of the Department. The NCIRP leverages the doctrine, capabilities, and organizing structures of the NRF, and both the NRF and NCIRP structures align with NIMS as described below.

NIMS provides the common language and incident management structure for government at all levels (federal and SLTT) and the private sector, and defines standard command and management structures. Successful response efforts, including cyber incident responses, depend on a common, interoperable approach for sharing resources, coordination, and communicating information. NIMS defines this comprehensive approach and enables the whole-of-Nation¹² to work together to prevent, protect against, mitigate, respond to, and recover from the effects of incidents regardless of cause, size, location, or complexity.

All of the components of the NIMS—resource management, management and coordination, and communications and information management—provide a common framework by which jurisdictions and organizations, which vary in authorities, management structures, communication capabilities, and protocols, integrate with one another to achieve common goals. These concepts can also apply to cyber incident response, in that they address:

- The development of a single set of incident objectives;
- The use of a collective, strategic approach to incident management;
- The improvement of information flow and coordination;
- The creation of a common understanding of joint priorities and limitations;
- The need to maintain an agency's legal authorities; and
- The optimization of the combined efforts of all participants in the incident.

The NRF also includes 14 Emergency Support Functions (ESF)¹³; these federal coordinating structures group resources and capabilities into functional areas that are most frequently needed in a national response. ESFs are an effective way to bundle and manage resources to deliver the core capabilities outlined in the NRF. These ESFs bring together the capabilities of federal departments and agencies and other national-level assets to support incident response. The ESFs are not based on

⁹ The NRF is one of five frameworks in the National Preparedness System; it describes how the whole community works together to achieve the National Preparedness Goal within the Response mission area.

<http://www.fema.gov/national-response-framework>.

¹⁰ <http://www.fema.gov/national-preparedness-goal>.

¹¹ 6 U.S.C. § 149

¹² The National Preparedness System refers to whole community vs the NCIRP describing a whole-of-Nation approach because of the nature of cyber infrastructure and associated incidents. The guidance, programs, processes, and systems that support each component of the National Preparedness System enable a collaborative, whole community approach to national preparedness that engages individuals, families, communities, private and nonprofit sectors, faith-based organizations, and all levels of government. <https://www.fema.gov/media-library-data/20130726-1855-25045-8110/national-preparedness-system-final.pdf>

¹³ <http://www.fema.gov/national-preparedness-resource-library>.

the capabilities of any single department or agency but are groups of organizations that work together to support an effective response.

Activation of the ESFs, either by the DHS Federal Emergency Management Agency (FEMA) or as directed by the Secretary of Homeland Security, depends upon the response activities needed to support the incident. Specifically, through ESF #2 (Communications), the Federal Government can coordinate the response to and recovery from a significant cyber incident that also creates large-scale physical effects with the communications sector and across the other ESFs. In an incident with cyber and physical effects, the significant cyber incident response mechanism outlined in the Coordinating Structures and Integration section of this Plan will coordinate with the established ESFs, to include ESF #2. A graphic comparing the Cyber Incident Severity Schema and Activation Level of the National Response Coordination Center is provided in Annex C. This center is a multiagency center that coordinates the overall federal support for major incidents and emergencies.¹⁴

The next section describes the concurrent lines of effort outlined in PPD-41 and identifies key roles and responsibilities for not only the federal and SLTT governments' response but also the private sectors' response to a cyber incident as they own and operate the bulk of the Nations' critical infrastructure.

Roles and Responsibilities

Every day, various organizations across the public and private sectors manage, respond to, and investigate cyber incidents through concurrent lines of effort. Fostering unity of effort during incident response requires a shared understanding of the roles and responsibilities of all participating organizations, to include roles that may be unique or particularly relevant for protecting the Nation from malicious cyber activity and managing cyber incidents and their consequences.

The Federal Government maintains a wide range of capabilities and resources that may be required to respond to a cyber incident, many of them through its cybersecurity centers which are further described in Annex E: Roles of Federal Cybersecurity Centers. In responding to any cyber incident and recognizing the shared responsibility for cybersecurity, the Federal Government organizes its' response activities based upon four concurrent lines of effort: threat response, asset response, intelligence support, and the affected entity's internal response activities.

When a cyber incident affects a private entity, the Federal Government will typically not play a direct role in the affected entities' response activities but will remain cognizant of their activities and coordinate appropriately with the affected entity. Where possible, and especially where incidents may escalate on the Cyber Incident Severity Schema, the Federal Government will conduct coordinated outreach efforts with the affected entity and offer to assist with asset response, threat response, and intelligence support activities, consistent with the guiding principles described in the Scope section of this Plan.

Cyber incidents can result from the actions, or inactions, of a single individual. When engaged and educated, individuals, families, and households can greatly reduce the impact, disruption, and damage caused by a cyber event. While most cyber incidents may not involve assistance from private citizens, incidents can reduce the risk and potential impact of a cyber incident to their personal property. Resources and guidance are available at www.ready.gov/cyber-attack that private citizens

¹⁴ The National Response Coordination Center. https://www.fema.gov/media-library-data/1440617086835-f6489d2de59dddeba8bebc9b4d419009/NRCC_July_2015.pdf

can leverage before, during, and after a cyber incident. US-CERT also provides information to home users on security risks and countermeasures associated with home Internet connectivity.¹⁵

Concurrent Lines of Effort

Recognizing the shared responsibility for cybersecurity, response activities in the NCIRP are undertaken through three concurrent lines of effort: threat response, asset response, intelligence support and related activities. A fourth line of effort is the affected entity's response efforts.¹⁶ These concurrent lines of effort provide a foundation for harmonizing various response efforts and fostering coordination and unity of effort before, during, and after any cyber incident response. Federal and non-federal entities should remain cognizant of these lines of effort and facilitate their activities accordingly while responding to cyber incidents.

Table 2. Lead Federal Agencies During Significant Cyber Incidents Affecting Civilian Networks¹⁷

Line of Effort	Lead Federal Agency
Threat Response	Department of Justice (DOJ) through the Federal Bureau of Investigation (FBI) and National Cyber Investigative Joint Task Force (NCIJTF)
Asset Response	Department of Homeland Security (DHS) through National Cybersecurity and Communications Integration Center (NCCIC)
Intelligence Support	Office of the Director of National Intelligence (ODNI) through Cyber Threat Intelligence Integration Center (CTIIC)
Affected Entity Response	When a significant cyber incident affects a federal agency, that agency will have primary responsibility for its response. When a significant cyber incident affects a private entity, the Federal Government will typically not play a role in this line of effort, but the cognizant Sector Specific Agency(ies) will generally coordinate the Federal Government efforts to understand the potential business or operational impact of a cyber incident on private sector critical infrastructure.

Threat and asset responders share some responsibilities and activities, including but not limited to:

- Communicating with the affected entity to understand the nature of the cyber incident;
- Providing guidance to the affected entity on available federal resources and capabilities;
- Promptly disseminating, through appropriate channels, intelligence and information learned in the course of the response; and
- Facilitating information sharing and operational coordination with other entities.

International coordination plays a key role through all the lines of effort. Due to the transnational nature of the Internet and communications infrastructure, and the global presence and connectivity of

¹⁵ <https://www.us-cert.gov/Home-Network-Security>

¹⁶ PPD-41: U.S. Cyber Incident Coordination. <https://www.whitehouse.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident>

¹⁷ Per the Annex to PPD-41, asset and threat response activities for significant cyber incidents affecting DoD or IC assets are led by those agencies with support from other federal agencies as appropriate. Lead agencies also coordinate with relevant SSAs, if a cyber incident affects or is likely to affect sectors they represent.

the U.S. private sector, the Federal Government may coordinate with international partners in response to all aspects of a cyber incident—threat response, asset response, and intelligence support.

The Department of State (DOS) represents the United States in all global diplomatic engagements across the full range of international policy imperatives, including cyber issues. As stated in the 2011 International Strategy for Cyberspace, diplomacy is a vital and necessary component to addressing cyber threats and responding to cyber incidents both domestically and internationally. DOS leverages its diplomats in the embassies and posts around the globe to provide international diplomatic support for cyber incident response around the clock. While DOS coordinates diplomatic outreach related to cyber incidents, many federal departments and agencies actively maintain and leverage multilateral and bilateral partnerships. Similarly, many ICT sector businesses and providers are multinational businesses with critical international elements and relationships, including interaction with both policy and operational communities around the world. As appropriate, federal departments and agencies collaborate internationally and with private sector entities to support international aspects of cyber incident response.

Threat Response

Threat response activities encompass many resources and capabilities from across the law enforcement and defense community. Threat response activities during a cyber incident include investigative, forensic, analytical, and mitigation activities; interdiction of a threat actor; and providing attribution that may lead to information sharing and operational synchronization with asset response activities. Threat response activities also include conducting appropriate law enforcement and national security investigative activities at the affected entity's site, linking related incidents, and identifying additional affected or potentially affected entities. As described earlier, threat responders and asset responders collaborate to foster a unity of effort to facilitate their activities while responding to incidents. The SLTT community and the private sector play important roles in working with respective law enforcement entities on threat response activities. Federal agencies with counterintelligence functions, such as those of DHS, DOJ, DoD, Department of Energy (DOE), and members of the Intelligence Community (IC), may perform a substantial threat response role when a significant cyber incident affects their duties or responsibilities, or there is suspicion of activities conducted a foreign power or agent of a foreign power.

Private Sector

Private sector entities perform critical roles in supporting threat response activities by reporting and sharing information regarding cyber incidents and malicious cyber activity in a timely manner to appropriate law enforcement agencies or government entities. Information, communications, and technology providers and manufacturers—such as Internet service providers, common carriers, manufacturers of key networking hardware, and major software companies—also play an important role in the threat response to malicious cyber activity, due to the potential exploitation or use of their systems by cyber threat actors. Points of contact for reporting incidents to Federal Government entities are provided in Annex D: Reporting Cyber Incidents to the Federal Government. Private sector entities should also adhere to regulatory and legal requirements when reporting cyber incidents. Private sector cybersecurity practitioners and providers that offer critical services (such as managed security services, indications and warning, cybersecurity assessment, and incident response) may also possess information concerning malicious cyber activity that is important to enable threat response activities. The *Cybersecurity Information Sharing Act of 2015* provides liability and other legal protections to private sector and certain SLTT government organizations and establishes

important conditions regarding sharing information with the Federal Government, SLTT government organizations, and the private sector.¹⁸

State, Local, Tribal, and Territorial Governments

Many states and locals have criminal statutes regarding unauthorized access or damage to computer systems, which could be implicated in a cyber incident. State fusion centers are situated at the intersection between federal and local law enforcement, and play a role in sharing threat-related information between federal, SLTT and/or private sector partners. However, state fusion centers vary greatly in their cyber capacity and capability. Local governments, particularly large cities, play an important role in local response activities. Often times, private citizens and small businesses do not have relationships with or access to federal law enforcement or in incident response activities. Local governments have a critical responsibility to provide a communication bridge to federal and state law enforcement and incident responders. As identified in the previous sub-section (Private Sector), the *Cybersecurity Information Sharing Act of 2015* establishes legal protections and important conditions for sharing information with the Federal Government, SLTT government organizations, and the private sector.

Federal Government

In response to cyber incidents, federal law enforcement agencies work across SLTT and the Federal Government, international engagements, and with private sector entities to address both criminal and national security cyber threats. Federal law enforcement agencies, such as the Federal Bureau of Investigation (FBI), United States Secret Service (U.S. Secret Service), and U.S. Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI), conduct threat response activities related to criminal activity involving their investigative jurisdictions and coordinate appropriately. Sharing action information in an unclassified format between the IC and first responders is critical in coordinating incident response activities.

Pursuant to PPD-41, during the event of a significant cyber incident for which a Cyber Unified Coordination Group (UCG) is convened, the DOJ, through the FBI and the National Cyber Investigative Joint Task Force (NCIJTF), will serve as the lead federal agency for threat response activities. The specific responsibilities and coordinating roles for this line of effort during a significant cyber incident are detailed in the Operational Coordination During a Significant Cyber Incident section of this Plan.

DOJ's Offices of U.S. Attorneys and its' Criminal and National Security Divisions, working with federal law enforcement agencies, use criminal and national security authorities to investigate, prosecute, and disrupt cyber threats and to apprehend cyber threat actors. Information and evidence obtained pursuant to appropriate legal process are used to identify the source of cyber incidents and to gather pertinent cyber threat information. Nationwide coordination of cyber prosecutorial initiatives is conducted through the DOJ Computer Hacking and Intellectual Property Program for criminal matters and by the DOJ National Security Cyber Specialist Network for cyber threats to the national security. In addition, DOJ, through the FBI and NCIJTF, shares investigative information and cyber threat intelligence, as appropriate, with other federal agencies to aid in the analysis of cyber threats and vulnerabilities. The FBI Cyber Task Forces in all 56 field offices support SLTT

¹⁸ Further information and guidance to assist non-federal entities to share cyber threat indicators and defensive measures with federal entities under the Cybersecurity Information Sharing Act of 2015 can be found at <https://www.us-cert.gov/ais>.

law enforcement in maintaining relationships and sharing information with the private sector, offering training and certification courses, and coordination of domestic cyber threat investigations.

The U.S. Secret Service has a national network of Electronic Crimes Task Forces, which combine the resources of academia, the private sector, and SLTT law enforcement to prevent, detect, and investigate electronic crimes, including potential terrorist attacks against critical infrastructure and financial payment systems.

DoD is responsible for threat response to cyber incidents affecting DoD assets and the DoD Information Network (DoDIN). DoD can also support civil authorities for cyber incidents outside the DoDIN when requested by the lead federal agency, and approved by the appropriate DoD official, or directed by the President. Such support would be provided based upon the needs of the incident, the capabilities required, and the readiness of available forces.

Asset Response

Asset response activities include furnishing technical assistance to affected entities, mitigating vulnerabilities, identifying additional at-risk entities, and assessing their risk to the same or similar vulnerabilities. These activities could also include communicating with the affected entity to understand the nature of the cyber incident; providing guidance to the affected entity on available federal, SLTT, and private sector resources and capabilities; promptly disseminating new intelligence and information through the appropriate channels; and facilitating information sharing and operational coordination with other Federal Government, SLTT government, and private sector entities. Critical asset response activities also include assessing potential risks to a sector or region, including potential cascading and interdependency effects, developing courses of action to mitigate these risks, and providing guidance on how best to utilize federal, SLTT, and private sector resources and capabilities in a timely, effective manner.

Asset and threat responders coordinate and share some responsibilities and activities when responding to a cyber incident. The roles and responsibilities in asset response vary, which highlights that unity of effort and shared responsibility is necessary to protect the Nation against cyber incidents.

Private Sector

The private sector, especially the owners and operators of critical infrastructure, plays a key role in responding to cyber incidents. Small, medium, and large private sector entities are often the first and primary responders to cyber incidents. Private companies are responsible for the security of their own systems, and they are normally the first to identify an incident and are often in the best place to respond to it. Private entities may have reporting or disclosure requirements related to cyber incidents, which they have to comply with as they respond to the incident. In most cases, these incidents are considered routine and are mitigated by the company using internal resources or with the assistance of contracted services providers. Routine, steady-state information sharing related to cyber incidents, even when mandatory reporting is not required, alerts other at-risk entities and allows them to mitigate vulnerabilities that may have cascading impacts to their systems.

Private sector service providers and cybersecurity practitioners offer critical services, such as managed security services, indications and warning, cybersecurity assessment, and incident response, which system owners and other asset responders might need when managing an incident. These private sector resources can serve as surge and specialty support to augment an in-house cybersecurity team at an affected entity.

Information, communications, and technology providers and manufacturers, such as Internet service providers, other common carriers, manufacturers of key networking hardware, and major software

companies, play an important role in defending against and responding to malicious cyber activity. Effective coordination between these private sector entities and other response organizations is often essential in cyber incident response.

Critical infrastructure owners and operators work with DHS and relevant sector-specific agencies (SSA) implementing the National Infrastructure Protection Plan (NIPP)¹⁹ tenets of public-private partnership to improve preparedness and manage risk. Due to the tightly interconnected and interdependent nature of some sectors, companies may also provide information to other entities in the sector or in other sectors, to facilitate shared situational awareness, contain the incident, and/or mitigate any damage. Thus, companies will potentially look to share and receive information from a variety of sources including DHS, SSAs, and federal and SLTT law enforcement and counterintelligence activities as well as their respective sector Information Sharing Analysis Centers (ISAC) and other information sharing and analysis organizations.

Most private sector operational information sharing is conducted through ISACs. ISACs are typically a sector-based type of Information Sharing and Analysis Organization (ISAO) and operate through a defined sector-based model, meaning that organizations within a certain sector (i.e. financial services, energy, aviation, etc.) join together to share information about cyber threats. Although many of these groups are already essential drivers of effective cybersecurity collaboration, some organizations do not fit neatly within an established sector or have unique needs. ISAOs can be formed based upon geography, sector, or any other grouping in which companies are interested and is a group created to gather, analyze, and disseminate cyber threat information. Those organizations that cannot join an ISAC but have a need for cyber threat information could benefit from membership in an ISAO. Unlike ISACs, ISAOs are not necessarily tied to critical infrastructure sectors.²⁰

In the case of cyber incidents, especially significant cyber incidents, greater coordination may be needed with the Federal Government, SLTT communities, regulators within the sector, and among multiple sectors. In addition to responding to situations in which private companies are themselves the victims of cyber incidents, private entities also respond to situations in which private sector service providers (especially Internet service providers, managed security service providers, and other technology vendors) provide support for national-level incident response efforts. During such an incident, the private sector often provides support or assistance to federal and SLTT departments and agencies on preparedness and response activities. Federal and SLTT regulators also have mandatory reporting requirements for certain types of cyber incidents in certain sectors. Depending on the sector and type of incident, some response actions may require regulator coordination, approval, and/or regulatory relief.

As appropriate, private sector entities provide for the security of their networks and security processing of breaches or other incidents through standing in-house or contracted services or use of external experts. Standing services are a part of the entity's network structure, and the private sector entity are encouraged share with government responders the information the standing services develop or pursue concerning a cyber incident. The *Cybersecurity Information Sharing Act of 2015* provides liability and other legal protections to private sector and certain SLTT government organizations and establishes important conditions regarding sharing information with the Federal Government, SLTT government organizations, and the private sector.²¹

¹⁹ NIPP, 2013. <https://www.dhs.gov/national-infrastructure-protection-plan>.

²⁰ <https://www.dhs.gov/isao-faq>

²¹ Further information and guidance to assist non-federal entities to share cyber threat indicators and defensive measures with federal entities under the Cybersecurity Information Sharing Act of 2015 can be found at <https://www.us-cert.gov/ais>.

State, Local, Tribal, and Territorial Government

Ensuring the safety and welfare of citizens is a fundamental responsibility of government at every level. Toward these objectives, key executives, executive leadership, elected officials, and executive staff of each SLTT government are responsible for ensuring preparedness, response, and recovery activities within their jurisdiction.

In cases of cyber incidents, the standard emergency response roles and responsibilities may not be sufficient to address technical challenges. Each state is responsible for developing a plan that describes their role in asset response for entities within their state. This state plan should be consistent with the NCIRP and serve as a cyber annex to their respective state emergency management plan. Information described in Annex G: Developing an Internal Cyber Incident Response Plan provides information each state can consider when developing a cyber incident response plan that coordinates identifying, detecting, mitigating, responding to, and recovering from cyber incidents in their state.

In establishing strong governance and reporting mechanisms, executives should identify key individual response points-of-contact for their respective governments and ensure the Federal Government has the most up-to-date information for these individuals. To facilitate coordination during a significant cyber incident response operation, each key executive should pre-designate a primary individual to serve as Senior Official to represent its government. Until amended, by each key executive, the NCCIC uses the state Homeland Security Advisors as its primary point of contact.

Governance is vital and an enabling factor in states' cyber asset response role. This includes the supporting legal framework, policies, plans, and procedures that codify the state chief information security officer's authorities and responsibilities. Governance also outlines how these relate to executive branch departments and agencies, and other state-operated entities to include (and not limited to) state and local emergency management functions, law enforcement, the judicial and legislative branches, ports, airports, and other state owned critical infrastructure. As identified in the previous sub-section (Private Sector), the *Cybersecurity Information Sharing Act of 2015* establishes legal protections and important conditions for sharing information with the Federal Government, SLTT government organizations, and the private sector.

Resources available to SLTT communities include, but are not limited to, the following:

- Regional Homeland Security Offices and Fusion Centers;
- Multi-State ISAC (MS-ISAC) is funded through grants from DHS to support the security of the SLTT government networks²² and acts as a focal point for critical information exchange and coordination between the SLTT community and the Federal Government; every state has an MS-ISAC primary member, usually the state chief information security officer (CISO);
- Local governments that are eligible to apply and receive Urban Area Security Initiative grant funds are encouraged to include cybersecurity and training programs as part of their expenditures.
- DHS National Protection and Programs Directorate field personnel, including:

²² The MS-ISAC does not help SLTT governments who are seeking to support the private sector. If an SLTT government is supporting a private sector company in asset response, the SLTT government should engage directly with the NCCIC.

- Supervisory, regional, and district-level Cybersecurity Advisors, who work closely with SLTT Chief Information Security Officers and cyber emergency management communities as cybersecurity subject matter experts;
- Regional directors and Protective Security Advisors, who work closely with state homeland security advisors as critical infrastructure protection specialists;
- The Governors Homeland Security Advisors Council, which provides a structure through which homeland security advisors from each state, territory, and the District of Columbia discuss homeland security issues, share information and expertise, and keep governors informed of the issues affecting homeland security policies in the states;
- The SLTT Government Coordinating Councils (SLTT GCC), which strengthen the sector partnership structure by bringing together geographically diverse experts from a wide range of critical infrastructure disciplines to ensure that SLTT officials play an integral role in national critical infrastructure security and resilience efforts.

The National Guard is a force with dual state and federal roles. National Guard forces have expertise in critical response functions and many also have expertise and capabilities in cyber activities. At the direction of a State Governor and Adjutant General, the National Guard may perform state missions, including supporting civil authorities in response to a cyber incident. In certain circumstances, as permitted by law, the National Guard may be requested to perform federal service or be ordered to active duty to perform DoD missions, which could include supporting a federal agency in response to a cyber incident.

Following a cyber incident, SLTT community leaders and points of contact may be asked to provide advice, support, and assistance to federal departments and agencies on preparedness and response activities related to SLTT priorities. Cyber incidents can cause cascading and/or physical impacts that implicate non-cyber incident response activities by SLTT governments. Key executives and points of contact have a need for situational awareness of the Federal Government's asset response activities even when a cyber incident does not affect the SLTT government systems. They should be prepared to request additional resources from the Federal Government—for instance, under the Stafford Act—in the event of a cyber incident that exceeds their government's capabilities.

Federal Government

Federal asset response to a significant cyber incident encompasses many resources and capabilities from across the federal departments and agencies as well as with the private sector. In response to cyber incidents, the Federal Government works with both domestic and foreign partners, including both private sector and governmental entities, to assist in assessments, mitigation, recovery, and restoration activities. Pursuant to PPD-41, in the event of a significant cyber incident for which a Cyber UCG is convened, DHS, through the NCCIC, will serve as the lead federal agency for asset response activities. The specific responsibilities and coordinating roles for this line of effort during a significant cyber incident are detailed in the Operational Coordination During a Significant Cyber Incident section of this Plan.

The Office of Management and Budget and the Federal Information Security Modernization Act of 2014 directs federal departments and agencies to report major cyber incidents within seven days as well as submitting to Congress, DHS, and Office of Management and Budget on an annual basis.²³

²³ Federal Information Security Modernization Act of 2014. Public Law No: 113-283. December 18, 2014. <https://www.congress.gov/bill/113th-congress/senate-bill/2521>

DHS, through the US-CERT, must be notified of all computer security incidents involving a Federal Government information system with a confirmed impact to confidentiality, integrity, or availability within one hour of being positively identified by the agency's top-level Computer Security Incident Response Team (CSIRT), Security Operations Center, or Information Technology department.²⁴

DHS provides strategic guidance, promotes a national unity of effort, and coordinates the overall federal effort to promote the security and resilience of the Nation's critical infrastructure from cyber and other threats.²⁵ Per the NCPA, DHS, through the NCCIC, serves as the federal civilian interface for sharing information related to cybersecurity risks, incidents, analysis, and warnings for federal and non-federal entities.²⁶ The NCCIC facilitates information sharing to help identify other entities at risk to the same or similar vulnerabilities and shares mitigation recommendations and best practices to protect those at risk. The NCCIC closely coordinates with the SSAs, representatives from multiple agencies, and the private sector to share cybersecurity information, information about risks and incidents, analysis, and warnings among federal and non-federal entities, and to facilitate coordination regarding cybersecurity risks and incidents across the civilian communities, SLTT governments, and the private sector. Federal asset response support to the private sector from the NCCIC in the form of on-site technical assistance is generally contingent on a request from or consent of the supported entity.

SSAs also play a role in sector coordination, working closely with DHS and serving as a day-to-day federal interface to prioritize and coordinate activities within their respective sectors; carrying out incident management responsibilities consistent with statutory authority and other appropriate policies, directives, or regulations; and providing support or facilitating technical assistance and consultations for that sector to identify vulnerabilities and help mitigate incidents, as appropriate. DHS ensures consistent and integrated approaches across various critical infrastructure sectors, and a nationwide approach including both unity of effort and unity of messages.

DHS, working with relevant SSAs, also coordinates the Government's efforts to understand the potential business or operational impact of a cyber incident on critical infrastructure in a given sector and across sectors. The relevant SSA will generally coordinate the Federal Government's efforts to understand the potential business or operational impact of a cyber incident on private sector critical infrastructure. SSAs receive support from the DHS NCCIC and the National Infrastructure Coordinating Center to maintain and provide situational awareness on threats, incidents, or events impacting critical infrastructure and to facilitate information sharing. This includes a near-real-time capability to provide SSA reports, coordinated with FEMA ESF reporting provided by the National Response Coordination Center, and the capability to solicit and receive information on incidents from public and private sector critical infrastructure partners. Because SSAs often have authorities, responsibilities, and partnerships with private industry that extend beyond security and resilience issues, SSAs play a lead role in integrating response to the technical aspects of cybersecurity incidents with efforts to mitigate the systemic impacts of such incidents to sectors.

²⁴ US-CERT Federal Incident Notification Guidelines. <https://www.us-cert.gov/incident-notification-guidelines>

²⁵ Presidential Policy Directive 21: Critical Infrastructure Security and Resilience. February 12, 2013. PPD-12 also assigns roles and responsibilities to other federal agencies. The Department of Justice and Federal Bureau of Investigation lead counterterrorism and counterintelligence investigations and related law enforcement activities across critical infrastructure. The Department of Homeland Security and the Attorney General collaborate to carry out their respective missions in critical infrastructure. <https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>

²⁶ The National Cybersecurity Protection Act of 2014. Public Law 113-282. December 18, 2014. <http://www.gpo.gov/fdsys/pkg/PLAW-113publ282/pdf/PLAW-113publ282.pdf>.

In responding to cyber incidents, DHS also works with foreign partners to exchange information and coordinate incident response activities. This international coordination principally occurs between the NCCIC and its foreign government CSIRT counterparts and builds on regular information sharing and operational coordination relationships. The DOC coordinates with federal, international, and private sector partners on the impacts of cyber incidents on the Internet ecosystem: the domain name system and the digital economy platform representatives to assess those impacts. Through the National Telecommunications and Information Administration and NIST, DOC serves as the Nation's authority on cybersecurity risk management practices and also fulfills responsibilities under the Defense Production Act²⁷ through the Bureau of Industry and Security, including support to critical infrastructure.

In some cases, regulatory or contract requirements could impose certain obligations on the affected entity related to asset response support, such as mandatory reporting requirements and/or national security determinations that may override normal consultative processes. Additionally, where they have relevant authority, federal regulators should be engaged early in the incident response process to ensure that actions requiring waiver or other approval or notification can be quickly executed. Regulators may also be able to facilitate coordinated actions of their respective sectors as necessary during significant cyber incidents.

DoD will be responsible for managing the asset response affected military assets and the DoDIN. DoD can also support civil authorities in responding to cyber incidents outside the DoDIN through a Defense Support of Civil Authorities request based upon a request by the lead federal agency and approved by the appropriate DoD official or directed by the President. Support would be provided based on the needs of the incident, the capabilities required, and the readiness of available forces.

When incidents affect IC assets, the IC Security Coordination Center (IC SCC) is responsible for asset response. The Office of the Director of National Intelligence (ODNI) manages the threat and asset response for the integrated defense of the IC information environment through the IC SCC, in conjunction with IC mission partners and with support from other federal agencies, as appropriate.

Intelligence Support

Intelligence and related supporting activities play an important role to better understand the cyber incident and existing targeted diplomatic, economic, or military capabilities to respond and share threat and mitigation information with other potential affected entities or responders. Especially during a significant cyber incident, asset and threat responders should leverage intelligence support activities as necessary to build situational threat awareness; share related threat indicators and analysis of threats; identify and acknowledge gaps; and ultimately create a comprehensive picture of the incident.

State, Local, Tribal, and Territorial Government

States fusion centers involve various levels of state government, private sector entities, and the public—though the level of involvement of some of these participants will vary based on specific circumstances. The fusion process should be organized and coordinated, at a minimum, on a statewide level, and each state should establish and maintain a center to facilitate the fusion process. Though the foundation of fusion centers is the law enforcement intelligence component, center leadership should evaluate their respective jurisdictions to determine what public safety and private sector entities should participate in the fusion center.

²⁷ Defense Production Act of 1950, as Amended October 2009. (50 U.S.C. App. 2061 et seq.)
<https://www.fema.gov/media-library/assets/documents/15666>

Federal Government

ODNI, through the Cyber Threat Intelligence Integration Center (CTIIC), provides intelligence support to federal agencies in response to cyber incidents. Pursuant to PPD-41, in the event of a significant cyber incident for which a Cyber UCG is convened, ODNI, through CTIIC, will serve as the lead federal agency for intelligence support and related activities. The specific responsibilities and coordinating roles for this line of effort during a significant cyber incident are detailed in the Operational Coordination During a Significant Cyber Incident section of this Plan.

In this role, CTIIC coordinates development of federal intelligence information for the other federal cybersecurity centers and federal stakeholders. This could include pursuing declassification of intelligence and/or “tear-line” reports at different classification levels as appropriate to the circumstances of the incident and overall U.S. equities. CTIIC also coordinates any intelligence collection activities that may take place as part of the incident through the National Intelligence Manager for Cyber.

Each intelligence operational center has its own organic intelligence support that aligns to its operational responsibilities. The DHS Office of Intelligence and Analysis has responsibilities under Title 6²⁸ to deliver intelligence to SLTT and private sector partners and develop intelligence from those partners for the Department and the IC. In addition, it provides intelligence support to the NCCIC’s private sector information sharing mission including gathering intelligence requirements from critical private sector companies and if the DHS National Protection and Programs Directorate concurs with the requirements can submit as formal requirements into the intelligence process.

The FBI collects and coordinates the sharing of relevant intelligence and other information between FBI domestic personnel and FBI staff assigned to Legal Attaché offices around the world; coordinates the sharing of intelligence among and between federal agencies and international intelligence and law enforcement elements; produces and shares analytical products, including those that assess threats to the homeland and inform related planning, capability development, and operational activities; and coordinates with ODNI mission and support centers that provide unique capabilities for homeland security partners.²⁹

The National Security Agency Cybersecurity Threat Operations Center (NCTOC) is the 24/7/365 NSA element that characterizes and assesses foreign cybersecurity threats. The NCTOC informs partners of current and potential malicious cyber activity through its analysis of foreign intelligence, with a focus on adversary computer network attacks, capabilities, and exploitations. Upon request, the NCTOC also provides technical assistance to U.S. Government departments and agencies.

The DoD actively characterizes and assesses foreign cybersecurity threats and informs the relevant interagency partners of current and potential malicious cyber activity. Upon request, the DoD intelligence components may provide technical assistance to U.S. Government departments and agencies; other DoD elements may provide support to civil authorities in accordance with applicable law and policy. The IC may identify classified information, indicating a potential credible cyber threat to an SLTT, critical infrastructure owner/operator, or other private sector entity. In accordance with Section 4 of Executive Order 13636, DHS and/or the FBI provide appropriate notification to the targeted entity.³⁰ Where available, declassified threat detection and mitigation information may also be provided. In circumstances where the source of threat identification, nature of the adversary, or

²⁸6 U.S.C. §124a.

²⁹ Title II of the Intelligence Reform and Terrorism Prevention Act of 2004, Public Law 108-458, 118 Stat. 3638, outlines FBI intelligence authorities, as does Executive Order 12333; 50 U.S.C. 401 et seq.; 50 U.S.C. 1801 et seq.”

³⁰ The NCIJTF has implemented the EO 13636 4(b) tracking system, Cyber Guardian, to record the production, dissemination, and disposition of these notifications.

other factors of national security concern exist, incident response processes and procedures adhere to all guidelines and directions for handling matters of national security.

Affected Entity's Response

Entities affected by a significant cyber incident usually undertake activities to manage the effects of the cyber incident on its operations, customers, and workforce, to include complying with various legal, regulatory, or contractual obligations. When a federal agency is an affected entity, that agency has primary responsibility for engaging in a variety of efforts to manage the impact of the cyber incident. These efforts could include, but not limited to:

- Maintaining business or operational continuity;
- Mitigating potential health and safety impacts;
- Addressing adverse financial impacts;
- Protecting privacy;
- Managing liability risk;
- Complying with legal and regulatory requirements (including disclosure and notification);
- Engaging in communications with employees or other affected individuals; and
- Managing external affairs (e.g., media and congressional inquiries).

When a cyber incident affects a private entity, the Federal Government typically will not play a role in this line of effort, but it will remain cognizant of the affected entity's response activities, consistent with the principles above and in coordination with the affected entity. The relevant SSA will generally coordinate the Federal Government's efforts to understand the potential business or operational impact of a cyber incident on private sector critical infrastructure.

Cyber Incidents Involving Personally Identifiable Information

As it relates to cyber incidents affecting civilian Federal Government agencies, if the facts and circumstances lead to a reasonable suspicion that the known or suspected cyber incident involves personally identifiable information, then the appropriate senior agency officials for privacy will be notified and lead any necessary personally identifiable information incident response process, as required by the Office of Management and Budget Memorandum M-07-1612, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* (and its subsequent revisions), and the agency's Breach Response Plan.³¹

Core Capabilities

Core capabilities are the distinct critical elements needed to conduct the threat response, asset response, and intelligence support activities in response to a cyber incident. Core capabilities are the activities that generally must be accomplished in cyber incident response, regardless of which levels of government are involved. They provide a common vocabulary to describe the significant functions that must be developed and executed across the whole-of-Nation to ensure preparedness.

³¹ Office of Management and Budget Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*. May 22, 2007.
<https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf>

Core capability application may be achieved with any combination of properly planned, organized, and trained personnel and deployed through various approaches such as the NIST Cybersecurity Framework or cybersecurity activities developed by the private sector. The National Preparedness Goal organizes the core capabilities into mission areas. These capabilities are aligned in Annex H: Core Capability/NIST Cybersecurity Framework/PPD-41 Crosswalk.

The capabilities are briefly described in this section and in further detail in Annex F: Core Capabilities and align with the National Preparedness Goal core capabilities.³² While Annex F is not an exhaustive list of capabilities, it provides a description of the capabilities that should be developed and utilized for particular needs, and roles, responsibilities, and authorities for the nature and scope of the cyber incident. All levels of government, private and non-profit sector organizations, and critical infrastructure owners and operators should assess their particular risks to identify their core capability requirements. Annex I describes additional resources that can be leveraged by both the private and public sector. Those resources can also serve as a starting point for understanding cyber incident response, vulnerability updates, data breach information, risk management, and organizations.

Responding to a cyber incident, like incident response for all other threats and hazards, is a shared responsibility. The whole-of-Nation must work together to ensure the United States is optimally prepared for cyber incidents; recognizing that not every network/system faces the same risks. By engaging the whole-of-Nation to build and deliver the cyber response core capabilities, the Nation is better prepared to respond to any threat or hazard, assist in restoring basic services and community functionality, and facilitate the integration of recovery activities.

Access Control and Identity Verification

Description: Apply and support necessary physical, technological, and cyber measures to control admittance to critical locations and systems, which is also referred to as Authentication and Authorization. This capability relies on the implementation and maintenance of protocols to verify identity and authorize, grant, or deny access to specific IT systems and networks.

Cybersecurity

Description: Protect (and, if needed, restore) computer networks, electronic communications systems, information, and services from damage, unauthorized use, and exploitation. More commonly referred to as information security, these activities ensure the security, reliability, confidentiality, integrity, and availability of critical information, records, and communications systems and services through collaborative initiatives and efforts.

Forensics and Attribution

Description: Forensic investigations and efforts to provide attribution for an incident are complementary functions that often occur in parallel during a significant cyber incident.

Forensics: Forensics is the term for discovering and identifying information relevant to an investigation through both scientific and intelligence-based acumen. In the context of a cyber incident, forensics refers to a number of technical disciplines related to the duplication, extraction, and analysis of data to uncover artifacts relevant to identifying malicious cyber activity. Forensics includes several sub-disciplines, including host-based forensics, network and packet data forensics,

³² <https://www.fema.gov/core-capabilities>

memory analysis, data correlation, and malware analysis.

During the response to a significant cyber incident, government agencies and private sector partners frequently conduct simultaneous analysis and share analytical results with each other to create a common understanding regarding the malicious cyber activity and how to defend against these or similar activity. In the days following an incident, a number of different threat, asset, and business response organizations may also engage in simultaneous forensic analysis. Although these lines of effort may appear to be duplicative, findings from these efforts could vary depending on the entities' varied access to particularized datasets or holdings.

Attribution: Attribution identifies an adversary linked to a particular incident. It is the culmination of the review of evidence and intelligence gathered during an incident which results in an assessment that identifies individuals or organizations which likely played a role in the cyber incident.

Attribution occurs over the lifecycle of an investigation and may not be known at the onset of a cyber incident response. Although the development of attribution for a significant cyber incident is one of the primary functions of lead federal response agencies, other government and private sector entities have a significant role to play in determining attribution.

An assessment regarding attribution for an incident is not only important for government agencies conducting criminal or national security investigations; it could also be significant to an affected entity as it considers whether to pursue additional legal or civil action against threat actors.

This core capability also includes unique and technical activities that support computer network and asset analysis during an incident. These supporting activities contribute to awareness of a comprehensive picture, which ultimately helps reduce the impact of a current incident and prevent future cyber incidents from spreading across the network.

Infrastructure Systems

Description: Stabilize critical infrastructure functions, minimize health and safety threats, and efficiently respond and recover systems and services to support a viable, resilient community following malicious cyber activity. Critical infrastructure and cyber networks are interdependent. In a response to a cyber incident, this capability focuses on stabilizing the infrastructure assets and entities, repairing damaged assets, regaining control of remote assets, and assessing potential risks to the critical infrastructure sector at large.

Intelligence and Information Sharing

Description: Provide timely, accurate, and actionable information resulting from the planning, direction, collection, exploitation, processing, analysis, production, dissemination, evaluation, and feedback of available information concerning threats of malicious cyber activity to the United States, its people, property, or interests. Intelligence and information sharing is the ability to exchange intelligence, information, data, or knowledge among government or private sector entities, as necessary.

In the context of a cyber incident, this capability involves the effective implementation of the intelligence cycle and other information collection and sharing processes by federal and SLTT entities, the private sector, and international partners to develop situational awareness of potential cyber threats to the United States.

Interdiction and Disruption

Description: Delay, divert, intercept, halt, apprehend, or secure threats related to malicious cyber activity. In the context of a cyber incident, these threats include people, software, hardware, or

activities that pose a threat to the Nation's cyber networks and infrastructure. This includes those interdiction and disruption activities that may be undertaken in response to specific, actionable intelligence of a cyber threat. Interdiction and disruption may include the targeting of persons, programs, or equipment or machines to stop or thwart threat activities and employing technical and other means to prevent malicious cyber activities. Interdiction and disruption capabilities help thwart emerging or developing cyber threats and neutralize operations. These capabilities should be utilized in a manner that preserves evidence and the Government's ability to prosecute those who violate the law.

Logistics and Supply Chain Management

Description: Facilitate and assist with delivery of essential commodities, equipment, and services in support of responses to systems and networks impacted by malicious cyber activity. Synchronize logistics capabilities and enable the restoration of impacted supply chains.

In the context of a cyber incident, this capability focuses on providing the logistical or operational support to achieve cyber incident response priorities established by leadership through identifying, prioritizing, and coordinating immediate response resource requirements.

Operational Communications

Description: Ensure the capacity for timely communications in support of security, situational awareness, and operations, by any and all means available, among and between entities affected by the malicious cyber activity and all responders.

In the context of a cyber incident, this capability includes identifying federal support organizations, capabilities, and teams with internal interoperable voice, video, and data systems and networks essential for effective cyber incident response operations. In a cyber incident, this capability focuses on the timely, dynamic, and reliable movement and processing of incident information in a form that meets the needs of decision makers at all levels of government and authorized participating private sector partner organizations.

Operational Coordination

Description: Establish and maintain a unified and coordinated operational structure and process that appropriately integrate all critical stakeholders and support execution of core capabilities. This is the capability to conduct actions and activities that enable decision makers across the whole-of-Nation to determine appropriate courses of action and to provide oversight for complex operations, to achieve unity of effort and effective outcomes. Operational coordination, in accordance with the principles of the NIMS and the Incident Command System, coordinates the threat response, asset response, and intelligence support activities in the face of a cyber threat or in response to an act of terrorism committed in the homeland. Unity of message is included within the guiding principles. Further information is available in Annex D: Reporting Cyber Incidents to the Federal Government.

In the context of a cyber incident, this core capability includes efforts to coordinate activities across and among all levels of government and with private sector partners. This capability involves national operations centers, as well as on-scene response activities that manage and contribute to multi-agency efforts.

Planning

Description: Conduct a systematic process engaging the whole-of-Nation, as appropriate, in the development of executable strategic, operational, and/or tactical-level approaches to meet defined

objectives.

In the context of a cyber incident, planning includes both deliberate planning and incident action planning. Deliberate planning involves developing strategic, operational, and tactical plans to prevent, protect against, mitigate the effects of, respond to, and recover from a cyber incident. Incident action planning occurs in a time-constrained environment to develop or rapidly adapt operational and tactical plans in response to an imminent or ongoing cyber incident.

Public Information and Warning

Description: Deliver coordinated, prompt, reliable, and actionable information to the whole-of-Nation and the public, as appropriate, through the use of clear, consistent, accessible, and culturally and linguistically appropriate methods to effectively relay information regarding significant threats or malicious cyber activity, as well as the actions being taken and the assistance being made available, as appropriate.³³

In the context of a significant cyber incident, this capability uses effective and accessible indications and warning systems to communicate significant cyber threats to involved or potentially involved operators, security officials, and the public (including alerts, detection capabilities, and other necessary and appropriate assets).

Screening, Search, and Detection

Description: Identify, discover, or locate threats of malicious cyber activity through active and passive surveillance and search procedures. This may include the use of systematic examinations and assessments, sensor technologies, or physical investigation and intelligence.

In the context of a cyber incident, this capability includes the measures which may be taken in response to actionable intelligence that indicates potential targets or types of malicious cyber activity, or the threat actors planning such activity. Measures may also be taken to verify or characterize a cyber threat that has already been located. Screening relative to a cyber incident may include monitoring the status of the network, assets, sensors, and other technologies that provide information on the security posture that may determine further action as necessary.

Situational Assessment

Description: Provide all decision makers with timely, decision-relevant information regarding the nature and extent of the malicious cyber activity, any cascading effects, and the status of the response.

In the context of a cyber incident, this capability focuses on rapidly processing and communicating large quantities of information from across the broader community, from the field level to the national level, to provide all decision makers with the most current and accurate information possible.

Threats and Hazards Identification

Description: Identify the threats of malicious cyber activity to networks and system; determine the frequency and magnitude of those threats; and incorporate this into analysis and planning processes

³³ The President of the United States has directed the Secretary of Homeland Security and the Attorney General to coordinate with each other to execute key responsibilities that provide public information and warning to the Nation regarding threats and incidents.

so as to clearly understand the needs of an entity.

In the context of a cyber incident, this capability involves the continual process of collecting timely and accurate data on cyber threats, including accounting for the future impacts of technology advancements, to meet the needs of analysts and decision makers. Effective Threats and Hazards Identification for a cyber incident is supported by standardized data sets, platforms, methodologies, terminologies, metrics, and reporting to unify levels of effort across all layers of government and the private sector, reducing redundancies.

Coordinating Structures and Integration

Successfully managing cyber incidents requires a whole-of-Nation approach (as described in the introduction of this document) that facilitates coordination among all stakeholders, including the private sector, SLTT governments, federal agencies, and international partners. Governing entities organize that coordination through established structures that promote unity of effort during incident response.

Coordinating structures provide a mechanism for representatives of entities that are affected by or are responsible for responding to a cyber incident to coordinate and facilitate response activities. These coordination and response activities may include preparedness activities, the delivery of capabilities, development operational plans, coordination of response personnel and activities, the crafting of unified public messaging and alerts, and weighing the technical, operational, political, and policy implications of varying courses of action.

While existing policies and coordinating structures can handle the vast majority of cyber incidents, significant cyber incidents may require a unique approach to coordinating the whole-of-Nation response. Pursuant to PPD-41, the U.S. Government will establish a Cyber UCG as the primary method for coordinating between and among federal agencies responding to a significant cyber incident, as well as for integrating SLTT governments and private sector partners into incident response efforts as appropriate for the specific incident. Other coordinating structures should be prepared to integrate and interoperate with a Cyber UCG, if one is established.

This section describes the major coordination structures in place across stakeholder communities that can be leveraged for response to cyber incidents requiring external coordination. Specifically, it describes how these structures will be leveraged, and additional structures incorporated, to provide operational coordination in response to significant cyber incidents.

Coordinating Structures

Stakeholders can utilize a variety of existing coordinating structures during any cyber incident to facilitate information sharing, coordinate response activities, access technical assistance and other resources, provide policy coordination and direction, and enable effective response. Most cyber incidents that occur on a daily basis are considered routine, and their responses are handled internally by the affected entity. As such, affected entities may choose to combine any of the coordinating structures below as deemed necessary to address the unique nature of the incident and specific organizational or sector needs. For significant cyber incidents, or cyber incidents that have implications for national security or public health and safety, PPD-41 establishes lead federal agencies and a coordinating structures framework with operational response planning and activities coordinated through a Cyber UCG.

Private Sector

For many years, the private sector has successfully engaged in coordination efforts between and across industry and government around detection, prevention, mitigation, and response to cyber

incidents through information sharing, analysis, and collaboration. Each of the 16 critical infrastructure sectors and sub-sectors designated under PPD-21: *Critical Infrastructure Security and Resilience*,³⁴ has a self-organized and self-governed Sector Coordinating Council (SCC). SCC members include critical infrastructure owners and operators, industry trade associations, and others across the private sector. SCCs provide a forum for members to engage with others across their sector, companion Government Coordinating Councils (GCCs), and SSAs to collaboratively address the full range of sector-specific and cross-sector critical infrastructure security and resilience policy and strategy efforts.

In addition, the private sector critical infrastructure community has developed its own coordination efforts through established ISACs. ISACs are based in and organized and governed by the private sector (with the exception of the MS-ISAC discussed later), with operational capabilities that support the public-private partnership around critical infrastructure protection and cybersecurity every day. The National Council of ISACs routinely facilitates cross-sector coordination to further productive engagement across the private sector and with government at the federal, state, and local levels.

As mentioned earlier, in accordance with policy established by Executive Order 13691, DHS is facilitating efforts to identify procedures to create and accredit ISAOs³⁵ to allow groups of stakeholders to create information sharing groups based on affinity among members (e.g., geography, industry or community segment, or threat exposure) that could provide a more formalized structure for information sharing and the provision of technical assistance. Some organizations, including those that are well established and delivering value every day, may be recognized as an ISAO and or ISAC, or as a member of more than one, concurrently. ISACs predate and are a subset of ISAOs.

State, Local, Tribal, and Territorial Governments

These levels of government also have a variety of coordination structures available to them for cyber incident response. These structures support information sharing, incident response, operational coordination, and collaboration on policy initiatives among participating governments.

As with private sector organizations, SLTT governments can be members of ISACs, ISAOs, or other information sharing organizations. They could also be members of the SLTT GCC at the national policy coordination level. For incidents on SLTT government networks MS-ISAC provides information sharing and technical assistance to its members and has established relationships with the Federal Government. As owners and operators of critical infrastructure and key resources, certain SLTT government agencies could also be members of sector-specific ISACs and may also develop unique structures, tailored to their jurisdiction's needs, to provide coordination and direction to response officials during a cyber incident. Many also collaborate with one another through selected cyber information sharing groups or organizations such as the National Association of State Chief Information Officers or the National Governors' Association.

While many SLTT governments are developing and utilizing operational coordination structures for cyber incident response, they have not all adopted a standard approach. Some may designate their state or major urban area fusion center as the primary contact and information sharing hub for cyber incident coordination while others could leverage their respective emergency or security operations center. For cyber incidents with physical effects, or that have consequences that must be managed in collaboration with other emergency management agencies (e.g., fire departments, public health agencies, human services offices), emergency operations centers will also likely provide important

³⁴ <https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>.

³⁵ www.isao.org

information sharing and incident management functions. At the state/territory level, emergency operations centers often coordinate resource requests with federal agencies, including FEMA and DoD, and provide operational coordination with the National Guard. The SLTT community are encouraged to provide cross-functional training in cybersecurity for the employees of their emergency operations center. As appropriate, cyber incident responders should also receive emergency response and emergency operations center training.

Federal Government

The Federal Government organizes coordinating structures into three categories for cyber incident response:

- National policy level coordination through the Cyber Response Group (CRG),³⁶
- Operational coordination through Federal Cybersecurity Centers and federal agencies, and
- Sector coordination through the SSAs and GCCs.

To coordinate policy at the National level, PPD-41 assigns the Assistant to the President for Homeland Security and Counterterrorism the responsibility to convene and chair the CRG to coordinate development and implementation of Federal Government policy and strategy with respect to significant cyber incidents affecting the Nation or its interests abroad. The CRG will coordinate the development and implementation of U.S. Government policy and strategy for responding to significant cyber incidents. Federal departments and agencies, including relevant cybersecurity centers, are invited to participate in the CRG, as appropriate, based on their respective roles, responsibilities, and expertise or in the circumstances of a given incident or grouping of incidents. Federal agencies, including SSAs that regularly participate in the CRG must establish and implement enhanced coordination procedures to manage significant cyber incidents that exceed their standing response capacities.

The Federal Government has established seven cybersecurity centers, with missions that include executing cyber operations, enhancing information sharing, maintaining situational awareness, and serving as conduits between public and private sector entities. Any or all of these centers should coordinate with federal entities and provide support to cyber incident response to the extent circumstances dictate and authorities permit. Pursuant to PPD-41, three of these centers coordinate significant cyber incident response activities within a Cyber UCG: the NCCIC, the NCIJTF, and CTIIC.

The Federal Government has also designated a number of SSAs to lead their sector GCCs, which are governmental counterparts to SCCs. SSAs are designated for each of the 16 critical infrastructure sectors designated under PPD-21. SSAs leverage their particular knowledge and expertise to fulfill a number of information sharing, coordination, incident response, and technical assistance responsibilities to their assigned critical infrastructure sector(s), as detailed in PPD-21 and the NIPP. GCCs include other government agencies with authorities and expertise in a given sector; robust engagement across GCC participants will enable interagency and interjurisdictional coordination by including broader participation from federal and SLTT governments, as appropriate to the needs of each sector.

³⁶ More information on the Cyber Response Group can be found within PPD-41: *U.S. Cyber Incident Coordination*. <https://www.whitehouse.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident-Annex-for-Presidential-Policy-Directive-41--United-States-Cyber-Incident-Coordination>. <https://www.whitehouse.gov/the-press-office/2016/07/26/annex-presidential-policy-directive-united-states-cyber-incident>.

International

International information sharing takes place through a variety of mechanisms in both the public and private sectors. Many organizations have information sharing relationships that extend to international partner companies and governments. International operational coordination can occur through relationships that federal departments and agencies have with their foreign counterparts and with international organizations, through formal diplomatic channels managed by DOS and through the relationships that private firms have internally, with other private sector entities, with national governments, and with international organizations.

Many federal agencies and cybersecurity centers have relationships with counterparts in foreign nations and routinely share information and collaborate, both during steady state and cyber incidents. Federal law enforcement agencies also maintain information sharing channels with foreign counterparts and the International Criminal Police Organization (INTERPOL) to facilitate international investigations. The FBI, through its Legal Attaché program, has designated Cyber liaison attaches stationed in U.S. Embassies. DHS/ICE HSI has broad legal authority to enforce a diverse array of federal statutes and uses this authority to investigate all types of cross-border criminal activity. The U.S. Secret Service maximizes partnerships with international law enforcement counterparts through overseas field offices and by forward deploying the Electronic Crimes Special Agent Program to international working groups. The NCCIC collaborates with international CSIRT partners to obtain situational awareness and determine priorities for protection and response. Organizations such as the DOS Overseas Security Advisory Council, for example, coordinates information sharing and collaborative security activity and analysis for U.S. private sector interests abroad through an industry representative council structure and established channels at U.S. embassies and other diplomatic posts. Additionally, some ISACs have chosen to open membership to firms and organizations located in friendly foreign nations, with safeguards in place to preserve confidentiality of information restricted to U.S. participants.

Given existing relationships and the overlapping policy and operational issues that may arise during a significant cyber incident, it is important to note that international coordination will likely occur through multiple channels concurrently.

Operational Coordination During a Significant Cyber Incident

Cyber incidents affect domestic stakeholders on an ongoing basis. The vast majority of these incidents pose no demonstrable risk to the U.S. national security interests, foreign relations, economy, public confidence, civil liberties, or public health and safety and thus do not rise to the designation of a significant cyber incident as defined by PPD-41 and the accompanying Cyber Incident Severity Schema in Annex B. Such cyber incidents are resolved either by the affected entity alone or with routine levels of support from, and in coordination with, other private sector stakeholders and/or from SLTT, federal, or international government agencies. In the event of a significant cyber incident, the Federal Government may form a Cyber UCG as the primary method for coordinating between and among federal agencies responding to a significant cyber incident and for integrating private sector partners into incident response efforts as appropriate.

Determination of Incident Severity

The Federal Government adopted the Cyber Incident Severity Schema in Annex B as a common framework and shared understanding to evaluate and assess cyber incidents at all federal departments and agencies when determining the severity of a cyber incident. Cyber incidents rated a “3” or greater will equate to a significant cyber incident. Federal Government departments and agencies shall leverage the Cyber Incident Severity Schema when assessing the severity level and the potential impact of cyber incidents to ensure common terminology, appropriate information sharing, and

proper management to effectively address an incident. As referenced earlier, Annex C compares the Cyber Incident Severity Schema and Activation Level of the National Response Coordination Center to demonstrate alignment cyber and physical incidents. When assessing the severity of a potentially significant incident, the federal cybersecurity centers that serve as lead federal agencies under PPD-41 (the NCCIC, NCIJTF, and CTIIC) will consult to make a joint assessment of severity.

Our Nation's critical infrastructure sectors are composed of public and private owners and operators, both of which provide vital services and possess unique expertise and experience that the Federal Government and Nation rely heavily upon. Therefore, when determining incident severity, DHS, through the NCCIC and the SSAs of sectors affected or likely to be affected, may consult with sector leadership and private sector owners and operators through organizations such as the sector ISAC(s), SCC, GCC, the National Council of ISACs, MS-ISAC, and/or the Partnership for Critical Infrastructure Security if the incident affects or is likely to affect a non-federal entity in one or more of the critical infrastructure sectors. The private sector assessment would inform the NCCIC severity rating of a cyber incident.

With the majority of critical infrastructure owned and operated by the private sector, it is more than likely that the Federal Government may learn of a potential significant cyber incident through voluntary self-reporting and information sharing from the affected entity or a sector coordinating mechanism. Non-federal entities are also encouraged to utilize the Cyber Incident Severity Schema and/or the NCCIC Cyber Incident Scoring System³⁷ to help organizations provide a repeatable and consistent mechanism for estimating the risk of an incident.

Additionally, when a significant cyber incident affects a private sector stakeholder, SLTT government, or international counterpart, they have several options for voluntarily sharing the issue with federal authorities including:

- The NCCIC, FBI, or NCIJTF;
- Applicable SSA(s) or regulators; or
- The local field office of federal law enforcement agencies, including the FBI, U.S. Secret Service, U.S. ICE/HSI, or relevant Military Criminal Investigative Organizations if defense related.

Points of contact for reporting incidents to Federal Government entities are provided in Annex D: Reporting Cyber Incidents to the Federal Government. In addition to voluntary reporting, affected entities that have mandatory reporting requirements according to law, regulation, or contract must continue to comply with such obligations.

The federal agency that receives the report will coordinate with other federal agencies in responding to the incident, including determining whether or not to establish a Cyber UCG to coordinate the response to the significant cyber incident. As a part of this determination, stakeholders can provide information and assessments to federal agencies regarding their view of the severity of the incident for their entity and for their sector. Federal agencies will leverage these assessments and engage with the affected entity for discussion as part of the decision process. As appropriate, the Federal Government also engages with relevant private sector organizations, ISACs, ISAOs, SCCs, SLTT governments, and/or international stakeholders for consultation about the severity and scope of the incident.

³⁷ National Cyber Incident Scoring System. <https://www.us-cert.gov/NCCIC-Cyber-Incident-Scoring-System>.

Enhanced Coordination Procedures

Per PPD-41, each federal agency that regularly participates in the CRG, including SSAs, ensures that it has the standing capacity to execute its role in cyber incident response. Agencies establish enhanced coordination procedures to prepare for significant cyber incidents that exceed its standing capacity. These procedures require dedicated leadership, supporting personnel, available facilities (physical and communications), and internal processes enabling it to manage a significant cyber incident under demands that would exceed its capacity to coordinate under normal operating conditions.

Enhanced coordination procedures help to:

- Identify the appropriate pathways for communicating with other federal agencies during a significant cyber incident, including the relevant agency points-of-contact, and for notifying the CRG that enhanced coordination procedures were activated or initiated;
- Highlight internal communications and decision-making processes that are consistent with effective incident coordination; and
- Outline processes for maintaining these procedures.

In addition, each federal agency's enhanced coordination procedures identify the agency's processes and existing capabilities to coordinate cyber incident response activities in a manner consistent with PPD-41. Government and private sector personnel should obtain the necessary clearances and accesses to facilitate the quick sharing of information. PPD-41 also directs SSAs to develop or update sector-specific procedures, as needed and in consultation with the sector(s), for enhanced coordination to support response to a significant cyber incident, consistent with this directive. These sector-focused procedures serve as a key mechanism for integrating government and private sector response processes, including processes for accounting for and responding to the business impacts of significant incidents.

Cyber UCG

A Cyber UCG, per PPD-41, serves as the primary national operational coordination mechanism between and among federal agencies responsible for identifying and developing operational response plans and activities during a significant cyber incident, as well as for integrating private sector partners and the SLTT communities into incident response efforts, as appropriate.

Authorities

The Cyber UCG works to establish shared objectives for threat response, asset response, and intelligence support to guide cyber incident response and recovery efforts in the short to mid-term. PPD-41 establishes the Cyber UCG and frames this concept of operations. PPD-41 does not alter, supersede, or limit the authorities of federal agencies to carry out their functions and duties consistent with applicable legal authorities and other Presidential guidance and directives. Instead, PPD-41 complements and builds upon PPD-8 on National Preparedness by integrating cyber and traditional preparedness efforts to manage incidents that include both cyber and physical effects. It also leverages the SSA construct and assignments of PPD-21 on Critical Infrastructure Security and Resilience. The Cyber UCG bolsters a unity of effort and does not alter agency authorities or leadership, oversight, or command responsibilities, unless mutually agreed upon between the relevant agency heads and consistent with applicable legal authorities, including the Economy Act of 1932.

Cyber UCG Formation

A Cyber UCG will be formed and activated only in the event of a significant cyber incident and will be incident specific. Cyber UCG will be formed by any of the following processes:

- At the direction of the National Security Council Principals Committee (Secretary level), Deputies Committee (Deputy Security level), or the CRG;
- When two or more federal agencies that generally participate in the CRG, including relevant SSAs, request its formation based on their assessment of the cyber incident against the severity schema; and or
- When a significant cyber incident affects critical infrastructure owners and operators identified by the Secretary of Homeland Security for which a cyber incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security

A Cyber UCG will dissolve when enhanced coordination procedures for threat and asset response are no longer required or the authorities, capabilities, or resources of more than one federal agency are no longer required to manage the remaining facets of the federal response to an incident.

Cyber UCG Responsibilities

Per PPD-41, a Cyber UCG conducts the following activities to promote unity of effort in response to a significant cyber incident:

- Coordinates the cyber incident response in a manner consistent with the principles described in the Section III of PPD-41 Annex;
- Ensures all appropriate federal agencies, including SSAs, are incorporated into the incident response;
- Coordinates the development and execution of response and recovery tasks, priorities, and planning efforts, including international and cross-sector outreach, necessary to respond appropriately to the incident and to speed recovery;
- Facilitates the rapid and appropriate sharing of information and intelligence among Cyber UCG participants on the incident response and recovery activities;
- Coordinates consistent, accurate, and appropriate communications regarding the incident to affected parties and stakeholders (and those who could be affected), including the public as appropriate; and
- For incidents that include cyber and physical effects, forms a combined UCG with the lead federal agency or with any UCG established to manage the physical effects of the incident under the NRF developed pursuant to PPD-8: *National Preparedness*,³⁸ or other applicable presidential policy directives.

The Cyber UCG will promptly coordinate with DOJ, general counsel from DHS, regulators, and other relevant federal agencies' attorneys about pertinent legal issues as they are identified to quickly consider and coordinate them with appropriate nongovernmental entities, as necessary.

³⁸ PPD-8, *National Preparedness*, March 30, 2011. <https://www.dhs.gov/xlibrary/assets/presidential-policy-directive-8-national-preparedness.pdf>.

Cyber UCG Participation

Per PPD-41, when a Cyber UCG is established, the Federal Government establishes three lead agencies to effectively respond to significant cyber incidents:

- DHS is the lead agency for **asset response** during a significant cyber incident, acting through the NCCIC. The NCCIC includes representation from the private sector, SLTT, and numerous federal agencies. It is a focal point for sharing cybersecurity information, information about risks and incidents, analysis, and warnings among federal and non-federal entities.
- DOJ is the lead agency for **threat response** during a significant cyber incident, acting through the FBI and the NCIJTF. Consisting of over 20 partner agencies from across law enforcement, the IC, and the DoD, the NCIJTF serves as a multi-agency focal point for coordinating, integrating, and sharing pertinent information related to cyber threat investigations.
- ODNI is the lead coordinator for **intelligence support** during a significant cyber incident, acting through the CTIIC. CTIIC provides situational awareness, sharing of relevant intelligence information, integrated analysis of threat trends, events, and support to interagency efforts to develop options to degrade or mitigate adversary threat capabilities. CTIIC also coordinates any intelligence collection activities that may take place as part of the incident, including identification of intelligence gaps, through the National Intelligence Manager, Cyber. Drawing upon the resources and capabilities across the Federal Government, the lead federal agencies are responsible for:
 - Coordinating any multi-agency threat or asset response activities to provide unity of effort, to include coordinating with any agency providing support to the incident, to include SSAs in recognition of their unique expertise;
 - Ensuring that their respective lines of effort are coordinated with other Cyber UCG participants and affected entities, as appropriate;
 - Identifying and recommending to the CRG, if elevation is required, any additional Federal Government resources or actions necessary to appropriately respond to and recover from the incident; and
 - Coordinating with affected entities on various aspects of threat, asset, and affected entity response activities through a Cyber UCG, as appropriate.

In addition to the lead federal agencies, a Cyber UCG will also include SSAs, if the cyber incident affects or is likely to affect sectors they represent as well as other federal cybersecurity centers as deemed necessary per the specific significant cyber incident. All federal agencies responding to the significant cyber incident will participate in, and coordinate their response activities with, a Cyber UCG.

SLTT government will be asked to participate in a Cyber UCG when the government entity owns or operates critical infrastructure that is or may be affected by that particular significant cyber incident. Otherwise, the Cyber UCG will use existing collaboration and information sharing mechanisms to provide regular updates to SLTT partners.

Like government participation, private sector involvement in a Cyber UCG will be limited to organizations with significant responsibility, jurisdiction, capability, or authority for response for that specific incident, which may not always include all organizations contributing resources to the response. Private Sector Cyber UCG participation will be voluntary and participants should be from organizations which can determine the incident priorities for each operational period and approve an Incident Action Plan, to include commitment of their organizations' resources to support execution of the Incident Action Plan. Per the Guiding Principles in PPD-41, out of respect for an affected

entities' privacy and sensitive private sector information, the Federal Government will coordinate with the affected entity on the approach of wider incident dissemination for that incident. Cyber UCG participants will be expanded or contracted as the situation changes during that particular incident response.

Depending on the nature and extent of the incident, a Cyber UCG might also incorporate specific ICT³⁹ companies, also known as ICT enablers, to directly assist on that specific incident response. ICT enablers are companies whose functions and capabilities are the foundations of the global cyber ecosystem. As such, it is these ICT enablers who are often best positioned to share information, ensure engagement of key players across the Internet and ICT realms, and assist with large-scale response efforts during a significant cyber incident.

Additionally, the Cyber UCG will continue to use several pre-existing and well-established coordinating structures, such as SCCs, ISACs and routine operational calls, for information sharing to ensure appropriate and timely sharing of actionable intelligence. As the operational arm for many sectors, ISACs especially can assist in their specific sector and across sectors impact assessment as the specific incident allows. Additional organizations may be engaged in response as participants in a Cyber UCG staff or as liaising organizations working in cooperation with the incident management team under separate leadership structures. Such organizations would generally have awareness of and opportunities to provide input to the Incident Action Plan, but would not be responsible for its contents or execution.

Regardless of specific participant composition, a Cyber UCG shall operate in a manner that is consistent with the need to protect intelligence and law enforcement sources, methods, operations, and investigations, the privacy of individuals, and sensitive and protected private sector information.

Information Sharing During Cyber Incident Response

Cyber UCGs share cyber threat information developed during incident response with other stakeholders as quickly, openly, and regularly as possible, to ensure protective measures can be applied with all applicable stakeholders. This sharing may at times be constrained by law, regulation, interests of the affected entity, classification or security requirements, or other operational considerations. However, participants will strive for unity of message when sharing with stakeholders and the public. Existing cyber threat information sharing channels will be used to disseminate such information where feasible.

In some cases, depending on how a Cyber UCG's participants have decided to staff a particular incident, this sharing could also take place via a Public Information Officer designated by the Cyber UCG or via a Joint Information Center staffed by representatives of responding organizations. In some cases, ad hoc information sharing mechanisms are required to provide effective situational awareness to interested or affected stakeholders. In all cases, Cyber UCGs protect the privacy of individuals and sensitive private sector information, as appropriate.

Conclusion

America's efforts to strengthen the security and resilience of networked technologies are never finished. To achieve this security and resilience, the public-private partnership is integral to collectively identifying priorities, articulating clear goals, mitigating risk, and adapting and evolving based on feedback and the changing environment. The Federal Government, SLTT governments, and

³⁹ The President's National Security Telecommunications Advisory Committee's Information Technology Mobilization Scoping Report. May 21, 2014. <https://www.dhs.gov/sites/default/files/publications/NSTAC%20-%20Information%20and%20Communications%20Technology%20Mobilization%20Report%2011-19-2014.pdf>

the Private and International partners remain resolute in its commitment to safeguard networks, systems and applications against the greatest cyber risks it faces, now and for decades to come.

The DHS Office of Cybersecurity and Communications will coordinate and oversee reviews and maintenance of the NCIRP in coordination with the DOJ, ODNI, and SSAs. The revision process includes developing or updating any documents necessary to carry out capabilities. Significant updates to the Plan will be vetted through a public-private senior-level review process. This Plan will be reviewed in order to accomplish the following:

- Assess and update information on the core capabilities in support of cyber and cyber-physical incident response goals and objectives.
- Ensure that it adequately reflects the organization of responsible entities.
- Ensure that it is compatible with doctrine and practices for the protection, prevention, mitigation, response, and recovery mission areas of the National Preparedness Goal.
- Update processes based on changes in the national threat/hazard environment.
- Incorporate lessons learned and effective practices from day-to-day operations, exercises, and actual incidents and alerts.
- Adapt to opportunities and challenges that arise as technology evolves and changes.
- Reflect progress in the Nation's cyber incident response mission activities, the need to execute new laws, executive orders, and Presidential directives, as well as strategic changes to national priorities and guidance, critical tasks, or national capabilities.

Additions or updates to the NCIRP annexes may occur independently from reviews of the base document based on lessons learned from immediate statute or law changes, cyber exercises or real world incidents.

Annex A: Authorities and Statutes

The authorities listed below provide the legal basis for Federal Government threat response, asset response, and intelligence support activities. Other laws and regulations place additional requirements on certain critical infrastructure sectors.

This list is not exhaustive, but it can be leveraged as a foundational resource.

- Communications Act of 1934, Section 706 (Public Law [PL] 73-416)
- Cybersecurity Act of 2015 (PL 114 – 113)
- Defense Production Act of 1950 (PL 81-744), as amended
- Executive Order (EO) 12333: *United States Intelligence Activities*, as amended
- EO 12382: *President’s National Security Telecommunications Advisory Committee*, as amended
- EO 12829: *National Industrial Security Program*, as amended
- EO 12968: *Access to Classified Information*, as amended
- EO 13549: *Classified National Security Information Programs for State, Local, Tribal, and Private Sector Entities*
- EO 13618: *Assignment of National Security and Emergency Preparedness Communications Functions*
- EO 13636: *Improving Critical Infrastructure Cybersecurity*
- EO 13691: *Promoting Private Sector Cybersecurity Information Sharing*
- Federal Information Security Modernization Act of 2014 (PL 113-283)
- Homeland Security Act of 2002 (as amended through Public Law 112-265)
- Homeland Security Presidential Directive (HSPD)-5: *Management of Domestic Incidents*
- Intelligence Authorization Act for Fiscal Year 2004 (PL 108-177)
- Intelligence Reform and Terrorism Prevention Act of 2004 (PL 108-458)
- National Cybersecurity Protection Act of 2014 (PL 113-282)
- National Infrastructure Protection Plan of 2013, *Partnering for Critical Infrastructure Security and Resilience*
- National Security Act of 1947 (PL 80-253), as amended
- National Security Directive 42: *National Policy for the Security of National Security Telecommunications and Information Systems*
- National Security Presidential Directive-54/ HSPD-23: *Cybersecurity Policy*
- Office of Management and Budget Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*.
- Presidential Policy Directive (PPD)-8: *National Preparedness*
- PPD-21: *Critical Infrastructure Security and Resilience*
- PPD-25: *U.S. Policy on Reforming Multilateral Peace Operations*
- PPD-40: *National Continuity Policy*

- PPD-41: *U.S. Cyber Incident Coordination Policy* and its accompanying Annex
- U.S. Code (USC) Title 6 – Domestic Security
- USC Title 10 – Armed Forces
- USC Title 18 – Crimes and Criminal Procedure
- USC Title 32 – National Guard
- USC Title 47 - Telecommunications
- USC Title 50 – War and National Defense

Annex B: Cyber Incident Severity Schema

Per Presidential Policy Directive (PPD)-41⁴⁰, the U.S. federal cybersecurity centers, in coordination with departments and agencies with a cybersecurity or cyber operations mission, adopted a common schema for describing the severity of cyber incidents affecting the homeland, U.S. capabilities, or U.S. interests. The schema establishes a common framework to evaluate and assess cyber incidents to ensure that all departments and agencies have a common view of the:

- Severity of a given incident;
- Urgency required for responding to a given incident;
- Seniority level necessary for coordinating response efforts; and
- Level of investment required for response efforts.

Figure 1 below depicts several key elements of the schema.

General Definition		Observed Actions	Intended Consequence ¹
Level 5 <i>Emergency</i> (Black)	<i>Poses an imminent threat to the provision of wide-scale critical infrastructure services, national gov't stability, or to the lives of U.S. persons.</i>	Effect	Cause physical consequence
Level 4 <i>Severe</i> (Red)	<i>Likely to result in a significant impact to public health or safety, national security, economic security, foreign relations, or civil liberties.</i>		Damage computer and networking hardware
Level 3 <i>High</i> (Orange)	<i>Likely to result in a demonstrable impact to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.</i>	Presence	Corrupt or destroy data Deny availability to a key system or service
Level 2 <i>Medium</i> (Yellow)	<i>May impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.</i>	Engagement	Steal sensitive information
Level 1 <i>Low</i> (Green)	<i>Unlikely to impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.</i>		Commit a financial crime
Level 0 <i>Baseline</i> (White)	Unsubstantiated or inconsequential event.	Preparation	Nuisance DoS or defacement

Figure 1: Elements of the Cyber Incident Severity Schema

⁴⁰ <https://www.whitehouse.gov/sites/whitehouse.gov/files/documents/Cyber+Incident+Severity+Schema.pdf>

Annex C: Cyber Incident Severity Schema/ National Response Coordination Center Activation Crosswalk

When incidents impact the cyber and/or physical environment(s), certain decisions and activities require coordination in order to respond in the most appropriate manner. The graphic below compares the Cyber Incident Severity Schema released in Presidential Policy Directive 41: United States Cyber Incident Coordination and the Department of Homeland Security National Response Coordination Center Activation Scale when comparing response levels for cyber and physical incidents.

Description	Disaster Level	Cyber Incident Severity	Description	Observed Actions
Due to its severity, size, location, actual or potential impact on public health, welfare, and infrastructure it requires an extreme amount of federal assistance for response and recovery efforts for which the capabilities to support do not exist at any level of government.	Level 1	Level 5 <i>Emergency</i>	Poses an imminent threat to the provision of wide-scale critical infrastructure services, national government security, or the lives of US citizens.	Effect
Requires elevated coordination among federal and SLTT governments due to moderate levels and breadth of damage. Significant involvement of FEMA and other federal agencies.	Level 2	Level 4 <i>Severe</i>	Likely to result in a significant impact to public health or safety, national security, economic security, foreign relations, or civil liberties.	Presence
		Level 3 <i>High</i>	Likely to result in a demonstrable impact to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.	
Requires coordination among federal and SLTT governments due to minor to average levels and breadth of damage. Typically, this is primarily a recovery effort with minimal response requirements.	Level 3	Level 2 <i>Medium</i>	May impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.	Engagement
		Level 1 <i>Low</i>	Unlikely to impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.	
No event or incident anticipated. This includes routine watch and warning activities.	Level 4	Level 0	Unsubstantiated or inconsequential event.	Steady State

Annex D: Reporting Cyber Incidents to the Federal Government¹

Cyber incidents can have serious consequences. The theft of private, financial, or other sensitive data and cyber incidents that damage computer systems are capable of causing lasting harm to anyone engaged in personal or commercial online transactions. Such risks are increasingly faced by businesses, consumers, and all other users of the Internet.

A private sector entity that is a victim of a cyber incident can receive assistance from Federal Government agencies, which are prepared to investigate the incident, help mitigate its consequences, and to help prevent future incidents. For example, federal law enforcement agencies have highly trained investigators who specialize in responding to cyber incidents for the express purpose of disrupting threat actors who caused the incident and preventing harm to other potential victims.

In addition to law enforcement, other federal responders provide technical assistance to protect assets, mitigate vulnerabilities, and offer on-scene response personnel to aid in incident recovery. When supporting affected entities, the various agencies of the Federal Government work in tandem to leverage their collective response expertise, apply their knowledge of cyber threats, preserve key evidence, and use their combined authorities and capabilities both to minimize asset vulnerability and bring malicious actors to justice. This Appendix explains when, what, and how to report to the Federal Government in the event of a cyber incident.

When to Report to the Federal Government. A cyber incident is an event that could jeopardize the confidentiality, integrity, or availability of digital information or information systems. Cyber incidents resulting in significant damage are of particular concern to the Federal Government. Accordingly, victims are encouraged to report all cyber incidents that may:

- Result in a significant loss of data, system availability, or control of systems;
- Impact a large number of victims;
- Indicate unauthorized access to, or malicious software present on, critical information technology systems;
- Affect critical infrastructure or core government functions; or
- Impact national security, economic security, or public health and safety.

The Federal Information Security Modernization Act of 2014 (FISMA) requires federal executive Branch civilian agencies to notify and consult with US-CERT regarding information security incidents involving their information and information systems, whether managed by a federal agency, contractor, or other source.

What to Report. A cyber incident may be reported at various stages, even when complete information is not available. Helpful information could include who you are, who experienced the incident, what sort of incident occurred, how and when the incident was initially detected, what response actions have already been taken, and who has been notified.

¹ This document was created in conjunction with Presidential Policy Directive 41 to provide the public with a unified federal message explaining how and when to report cyber incidents for purposes of obtaining assistance from the Federal Government. It does not address mandatory reporting pursuant to law, regulation, or contract. Such required reporting should continue to occur through designated federal points of contact using existing procedures.

How to Report Cyber Incidents to the Federal Government. Private sector entities experiencing cyber incidents are encouraged to report a cyber incident to the local field offices of federal law enforcement agencies, their sector specific agency, or any of the federal agencies listed in Table 1 below. The federal agency receiving the initial report will coordinate with other relevant federal stakeholders to respond to the incident. If the affected entity is obligated by law or contract to report a cyber incident, the entity should comply with that obligation, in addition to voluntarily reporting the incident to an appropriate federal point of contact. Federal agencies also collaborates with state, local, territorial and tribal government organizations as appropriate given the nature of the cyber incident.

Types of Federal Incident Response. Upon receiving a report of a cyber incident, the Federal Government will promptly focus its efforts on two activities: threat response and asset response:

- **Threat response** includes attributing, pursuing, and disrupting malicious cyber actors and malicious cyber activity. It includes conducting criminal investigations and other actions to counter the malicious cyber activity.
- **Asset response** includes protecting assets and mitigating vulnerabilities in the face of malicious cyber activity. It includes reducing the impact to systems and/or data; strengthening, recovering and restoring services; identifying other entities at risk; and assessing potential risk to the broader community and mitigating potential privacy risks to affected individuals.

Irrespective of the type of incident or its corresponding response, federal agencies work together to help affected entities understand the incident, link related incidents, and share information to rapidly resolve the situation in a manner that protects privacy and civil liberties.

Table 1: Key Federal Points of Contact

Threat Response	Asset Response
Federal Bureau of Investigation (FBI): FBI Field Office Cyber Task Forces: http://www.fbi.gov/contact-us/field Internet Crime Complaint Center (IC3): http://www.ic3.gov ▪ Report cybercrime, including computer intrusions or attacks, fraud, intellectual property theft, identity theft, theft of trade secrets, criminal hacking, terrorist activity, espionage, sabotage, or other foreign intelligence activity to FBI Field Office Cyber Task Forces. ▪ Report individual instances of cybercrime to the IC3, which accepts Internet crime complaints from both victim and third parties.	National Cybersecurity and Communications Integration Center (NCCIC) (888) 282-0870 or NCCIC@hq.dhs.gov United States Computer Emergency Readiness Team: http://www.us-cert.gov ▪ Report suspected or confirmed cyber incidents, including when the affected entity may be interested in government assistance in removing the adversary, restoring operations, and recommending ways to further improve security.
National Cyber Investigative Joint Task Force (NCIJTF) CyWatch 24/7 Command Center: cywatch@ic.fbi.gov or (855) 292-3937 ▪ Report cyber intrusions and major cybercrimes that require assessment for action, investigation, and engagement with local field offices of federal law enforcement agencies or the Federal Government.	

Threat Response	Asset Response
United States Secret Service (USSS) Secret Service Field Offices and Electronic Crimes Task Forces (ECTFs): http://www.secretservice.gov/contact/field-offices ▪ Report cybercrime, including computer intrusions or attacks, transmission of malicious code, password trafficking, or theft of payment card or other financial payment information.	
United States Immigration and Customs Enforcement / Homeland Security Investigations (ICE/HSI) HSI Tip Line: 866-DHS-2-ICE (866-347-2423) or www.ice.gov/webform/hsi-tip-form HSI Field Offices: https://www.ice.gov/contact/hsi HSI Cyber Crimes Center: https://www.ice.gov/cyber-crimes ▪ Report cyber-enabled crime, including: digital theft of intellectual property; illicit e-commerce (including hidden marketplaces); Internet-facilitated proliferation of arms and strategic technology; child pornography; and cyber-enabled smuggling and money laundering.	

If there is an immediate threat to public health or safety, the public should always call 911.

Annex E: Roles of Federal Cybersecurity Centers

The Federal Government has established a number of cybersecurity centers associated with various departments and agencies to execute operational missions, enhance information sharing, maintain situational awareness of cyber incidents, and serve as conduits between public-and private-sector stakeholder entities. In support of the Federal Government’s coordinating structures on cyber incident management, a Cyber Unified Coordination Group⁴¹ may elect to leverage these cybersecurity centers for their established enhanced coordination procedures, above-steady-state capacity, and/or operational or support personnel.

National Cybersecurity and Communications Integration Center (NCCIC)

As an operational element of the Department of Homeland Security, the NCCIC is the primary platform to coordinate the Federal Government’s asset response to cyber incidents. The NCCIC is authorized under Section 3 of the National Cybersecurity Protection Act of 2014.

National Cyber Investigative Joint Task Force (NCIJTF)

The NCIJTF is a multi-agency center hosted by the Federal Bureau of Investigation and is the primary platform to coordinate the Federal Government’s threat response. The NCIJTF is chartered under paragraph 31 of National Security Presidential Directive-54/Homeland Security Presidential Directive-23.

Cyber Threat Intelligence Integration Center (CTIIC)

Operated by the Office of the Director of National Intelligence, the CTIIC is the primary platform for intelligence integration, analysis, and supporting activities for the Federal Government. CTIIC also provides integrated all-source analysis of intelligence related to foreign cyber threats or related to cyber incidents affecting U.S. national interests.

U.S. Cyber Command (USCYBERCOM) Joint Operations Center (JOC)

The USCYBERCOM JOC directs the U.S. military’s cyberspace operations and defense of the Department of Defense Information Network (DoDIN). USCYBERCOM manages both the threat and asset responses for the DoDIN during incidents affecting the DoDIN and receives support from the other centers, as needed.

National Security Agency Cybersecurity Threat Operations Center (NCTOC)

The National Security Agency Cybersecurity Threat Operations Center (NCTOC) is the 24/7/365 NSA element that characterizes and assesses foreign cybersecurity threats. The NCTOC informs partners of current and potential malicious cyber activity through its analysis of foreign intelligence, with a focus on adversary computer network attacks, capabilities, and exploitations. Upon request, the NCTOC also provides technical assistance to U.S. Government departments and agencies.

Department of Defense Cyber Crime Center (DC3)

DC3 supports the law enforcement, counterintelligence, information assurance, network defense, and critical infrastructure protection communities through digital forensics, focused threat analysis, and training. DC3 provides analytical and technical capabilities to federal agency mission partners conducting national cyber incident response.

⁴¹ See page 30 for description.

Intelligence Community – Security Coordination Center (IC-SCC)

The IC-SCC mission is to monitor and oversee the integrated defense of the IC Information Environment in conjunction with IC mission partners and in accordance with the authority and direction of the Office of the Director of National Intelligence Chief Information Officer. The IC - Incident Response Center roles and responsibilities were assumed upon the IC SCC's founding in 2014.

Annex F: Core Capabilities and Critical Tasks

Each core capability identified in the National Cyber Incident Response Plan (NCIRP) has critical tasks that facilitate capability execution. These critical tasks are tasks that are essential to achieving the desired outcome of the capability. Critical tasks inform mission objectives, which allow planners to identify resourcing and sourcing requirements prior to an incident. The chart below describes each core capability and identifies critical tasks associated with each capability.

Core Capabilities and Critical Tasks
1. <u>Access Control and Identity Verification</u> Description: Apply and support necessary physical, technological, and cyber measures to control admittance to critical locations and systems. Also referred to as Authentication and Authorization. Critical Tasks: • Verify identity to authorize, grant, or deny access to cyber assets, networks, applications, and systems that could be exploited to do harm. • Control and limit access to critical locations and systems to authorized individuals carrying out legitimate activities. • Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties. • Perform audit activities to verify and validate security mechanisms are performing as intended. • Conduct training to ensure staff-wide adherence to access control authorizations.
2. <u>Cybersecurity</u> Description: Protect (and, if needed, restore) computer networks, electronic communications systems, information, and services from damage, unauthorized use, and exploitation. More commonly referred to as computer network defense, these activities ensure the security, reliability, confidentiality, integrity, and availability of critical information, records, and communications systems and services through collaborative initiatives and efforts. Critical Tasks: • Implement countermeasures, technologies, and policies to protect physical and cyber assets, networks, applications, and systems that could be exploited. • Secure, to the extent possible, public and private networks and critical infrastructure (e.g., communication, financial, electricity sub-sector, water, and transportation systems), based on vulnerability results from risk assessment, mitigation, and incident response capabilities. • Create resilient cyber systems that allow for the uninterrupted continuation of essential functions. • Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties. • Respect defined limitations and frontiers of cybersecurity policy among collaborative security partners.

Core Capabilities and Critical Tasks

3. Forensics and Attribution

Description: Forensic investigations and efforts to provide attribution for an incident are complementary functions that often occur in parallel during a significant cyber incident.

Critical Tasks:

- Retrieve digital media and data network security and activity logs.
- Conduct digital evidence analysis, and respecting chain of custody rules.
- Conduct physical evidence collections, analysis adhere to rules of evidence collection as necessary.
- Assess capabilities of likely threat actors(s).
- Leverage the work of incident responders and technical attribution assets to identify malicious cyber actor(s).
- Interview witnesses, potential associates, and/or perpetrators if possible.
- Apply confidence levels to attribution assignments.
- Include suitable inclusion and limitation information for sharing products in attribution elements guidance.
- Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties.
- Perform audit activities to verify and validate security mechanisms are performed as intended.

4. Infrastructure Systems

Description: Stabilize critical infrastructure functions, minimize health and safety threats, and efficiently respond and recover systems and services to support a viable, resilient community following malicious cyber activity.

Critical Tasks:

- Maintain a comprehensive understanding of the needs for the safe operation of control systems.
- Stabilize and regain control of infrastructure.
- Increase network isolation to reduce the risk of a malicious cyber activity propagating more widely across the enterprise or among interconnected entities.
- Stabilize infrastructure within those entities that may be affected by cascading effects of the cyber incident.
- Facilitate the restoration and sustainment of essential services (public and private) to maintain community functionality.
- Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties.
- Maintain up-to-date data knowledge of applicable emerging and existing security research, development, and solutions.

Core Capabilities and Critical Tasks

5. Intelligence and Information Sharing

Description: Provide timely, accurate, and actionable information resulting from the planning, direction, collection, exploitation, processing, analysis, production, dissemination, evaluation, and feedback of available information concerning threats of malicious cyber activity to the United States, its people, property, or interests. Intelligence and information sharing is the ability to exchange intelligence, information, data, or knowledge among government or private sector entities, as necessary.

Critical Tasks:

- Monitor, analyze, and assess the positive and negative impacts of changes in the operating environment as it pertains to cyber vulnerabilities and threats.
- Share analysis results through participation in the routine exchange of security information—including threat assessments, alerts, threat indications and warnings, and advisories—among partners.
- Confirm intelligence and information sharing requirements for cybersecurity stakeholders.
- Develop or identify and provide access to mechanisms and procedures for confidential intelligence and information sharing between the private sector and government cybersecurity partners.⁴²
- Use intelligence processes to produce and deliver relevant, timely, accessible, and actionable intelligence and information products to others as applicable, to include critical infrastructure participants and partners with roles in physical response efforts.
- Share actionable cyber threat information with SLTT and international governments and private sectors to promote shared situational awareness.
- Enable collaboration via online networks that are accessible to all participants.
- Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties.

⁴² Information sharing must provide effective communication to individuals with access and functional needs, including people with limited English proficiency and people with disabilities, including people who are deaf or hard of hearing and people who are blind or have low vision. Effective communication with individuals with access and functional needs includes use of appropriate auxiliary aids and services, such as sign language and other interpreters, captioning of audio and video materials, user-accessible Web sites, communication in various languages, and use of culturally diverse media outlets.

Core Capabilities and Critical Tasks

6. Interdiction and Disruption

Description: Delay, divert, intercept, halt, apprehend, or secure threats related to malicious cyber activity.

Critical Tasks:

- Deter malicious cyber activity within the United States, its territories, and abroad.
- Interdict persons associated with a potential cyber threat or act.
- Deploy assets to interdict, deter, or disrupt cyber threats from reaching potential target(s).
- Leverage law enforcement and intelligence assets to identify, track, investigate, and disrupt malicious actors threatening the security of the Nation's public and private information systems.
- Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties.
- Respect defined limitations and frontiers of cybersecurity policy among collaborative security partners.

7. Logistics and Supply Chain Management

Description: Facilitate and assist with delivery of essential commodities, equipment, and services to include the sustainment of responders in support of responses to systems and networks impacted by malicious cyber activity. Synchronize logistics capabilities and enable the restoration of impacted supply chains.

Critical Tasks:

- Identify and catalog resources needed for response, prior to mobilization.
- Mobilize and deliver governmental, nongovernmental, and private sector resources to stabilize the incident and integrate response and recovery efforts, to include moving and delivering resources and services to meet the needs of those impacted by a cyber incident.
- Facilitate and assist delivery of critical infrastructure components to rapid response and restoration of cyber systems.
- Enhance public and private resource and services support for impacted critical infrastructure entities.
- Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties.
- Apply supply chain assurance principles and knowledge within all critical tasks identified above.

Core Capabilities and Critical Tasks

8. Operational Communications

Description: Ensure the capacity for timely communications in support of security, situational awareness, and operations, by any and all means available, among and between entities affected by the malicious cyber activity and all responders.

Critical Tasks:

- Ensure the capacity to communicate with both the cyber incident response community and the affected entity.
- Establish interoperable and redundant voice, data, and broader communications pathways between SLTT, particularly state fusion centers, federal, and private sector cyber incident responders.
- Facilitate establishment of quickly formed ad hoc voice and data networks on a local and regional basis so critical infrastructure entities can coordinate activities even if Internet services fail.
- Coordinate with any UCG (or entity) established to manage physical (or non-cyber) effects of an incident. Ensure availability of appropriate secure distributed and scalable incident response communication capabilities including out-of-band communications mechanisms where traditional communications and/or systems are compromised. Adhere to appropriate mechanisms for safeguarding sensitive and classified information private sector personnel should obtain the necessary clearances and accesses to facilitate the quick sharing of information.
- Protect individual privacy, civil rights, and civil liberties.
- Cyber threat information also is conducted through automated indicator sharing using established formats such as Structured Threat Information eXpression/Trusted Automated eXchange of Indicator Information (STIX/TAXII).⁴³
- Perform red team activities to verify and validate that forensics and attribution capabilities are performing as intended and have adequate visibility.

9. Operational Coordination

Description: Establish and maintain a unified and coordinated operational structure and process that appropriately integrate all critical stakeholders and support execution of core capabilities.

Critical Tasks:

- Mobilize all critical resources and establish coordination structures as needed throughout the duration of an incident.
- Define and communicate clear roles and responsibilities relative to courses of action.
- Prioritize and synchronize actions to ensure unity of effort.
- Ensure clear lines and modes of communication between entities, both horizontally and vertically.
- Ensure appropriate private sector participation in operational coordination throughout the cyber incident response cycle consistent with the NIPP.
- Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties.
- Perform table-top activities to verify and validate effective and appropriate coordination between stakeholders.

⁴³ <https://www.us-cert.gov/Information-Sharing-Specifications-Cybersecurity>

Core Capabilities and Critical Tasks

10. Planning

Description: Conduct a systematic process engaging the whole community, as appropriate, in the development of executable strategic, operational, and/or tactical-level approaches to meet defined objectives.

Critical Tasks:

- Initiate a flexible planning process that builds on existing plans as part of the National Planning System.⁴⁴
- Collaborate with partners to develop plans and processes to facilitate coordinated incident response activities.
- Establish partnerships that coordinate information sharing between partners to restore critical infrastructure within single and across multiple jurisdictions and sectors.
- Inform risk management response priorities with critical infrastructure interdependency analysis.
- Identify and prioritize critical infrastructure and determine risk management priorities.
- Conduct cyber vulnerability assessments, perform vulnerability and consequence analyses, identify capability gaps, and coordinate protective measures on an ongoing basis in conjunction with the private and nonprofit sectors and local, regional/metropolitan, state, tribal, territorial, insular area, and federal organizations and agencies.
- Develop operational, business/service impact analysis, incident action, and incident support plans at the federal level and in the states and territories that adequately identify critical objectives based on the planning requirements; provide a complete and integrated picture of the escalation and de-escalation sequence and scope of the tasks to achieve the objectives; and are implementable within the time frame contemplated in the plan using available resources.
- Formalize partnerships such as memorandums of understanding or pre-negotiated contracts with governmental and private sector cyber incident or emergency response teams to accept, triage, and collaboratively respond to incidents in an efficient manner.
- Formalize partnerships between communities and disciplines responsible for cybersecurity and for physical systems dependent on cybersecurity. Formalize relationships such as memorandums of understanding or pre-negotiated contracts between information communications technology and information system vendors and their customers for ongoing product cyber security, business planning, and transition to response and recovery when necessary.
- Formalize partnerships with government and private sector entities for data and threat intelligence sharing, prior to, during, and after an incident.
- Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties.

⁴⁴ The National Planning System provides a unified approach and common terminology to support the implementation of the [National Preparedness System](#) through plans that support an “all threats and hazards” approach to preparedness. These plans—whether strategic, operational, or tactical—enable the whole community to build, sustain, and deliver the core capabilities identified in the [National Preparedness Goal](#).

Core Capabilities and Critical Tasks

11. Public Information and Warning

Description: Deliver coordinated, prompt, reliable, and actionable information to the whole community and the public, as appropriate, through the use of clear, consistent, accessible, and culturally and linguistically appropriate methods to effectively relay information regarding significant threat or malicious cyber activity, as well as the actions being taken and the assistance being made available, as appropriate.

Critical Tasks:

- Establish accessible mechanisms and provide the full spectrum of support necessary for appropriate and ongoing information sharing among all levels of government, the private sector, faith-based organizations, nongovernmental organizations, and the public.
- Share actionable information and provide situational awareness with the public, private, and nonprofit sectors, and among all levels of government.
- Leverage all appropriate communication means, such as the Integrated Public Alert and Warning System, public media, and social media sites.
- Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties.
- Respect applicable information sharing and privacy protections, including Traffic Light Protocol.
- Assure availability of redundant options to achieve critical public information, threat indication, and warning outcomes.

12. Screening, Search, and Detection

Description: Identify, discover, or locate threats of malicious cyber activity through active and passive surveillance and search procedures. This may include the use of systematic examinations and assessments, sensor technologies, or physical investigation and intelligence.

Critical Tasks:

- Locate persons and networks associated with cyber threats.
- Develop relationships and further engage with critical infrastructure participants (private industry and SLTT partners).
- Conduct physical and electronic searches as authorized by law
- Collect and analyze information provided.
- Detect and analyze malicious cyber activity and support mitigation activities.
- Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties.
- Respect defined limitations and frontiers of cybersecurity policy among collaborative security partners.

Core Capabilities and Critical Tasks

13. Situational Assessment

Description: Provide all decision makers with decision-relevant information regarding the nature and extent of the malicious cyber activity, any cascading effects, and the status of the response.

Critical Tasks:

- Coordinate the production and dissemination of modeling and effects analysis to inform immediate cyber incident response actions.
- Maintain standard reporting templates, information management systems, essential elements of information, and critical information requirements.
- Develop a common operational picture for relevant incident information shared by more than one organization.
- Coordinate the structured collection and intake of information from multiple sources for inclusion into the assessment processes.
- Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties.

14. Threats and Hazards Identification

Description: Identify the threats of malicious cyber activity to networks and system; determine the frequency and magnitude; and incorporate this into analysis and planning processes so as to clearly understand the needs of an entity.

Critical Tasks:

- Identify data requirements across stakeholders.
- Develop and/or gather required data in a timely and efficient manner to accurately identify cyber threats.
- Ensure that the right people receive the right data at the right time.
- Translate data into meaningful and actionable information through appropriate analysis and collection tools to aid in preparing the public.
- Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties.
- Discover, evaluate and resolve gaps in policy, facilitate or enable technologies, partnerships, and procedures which are barriers to effective threat, vulnerability, and hazard identification for the sectors.

Annex G: Developing an Internal Cyber Incident Response Plan

This Annex describes processes that may be used for cyber incident response planning. The first subsection describes the national operational planning process. The second subsection outlines a planning process that individual entities may take.

National Operational Planning

An operational plan is a continuous, evolving instrument of anticipated actions that maximizes opportunities and guides response operations. Operational plans are “living documents,” subject to revision as incidents evolve and new information becomes available. Operational plans seek to:

- Improve coordination, collaboration, and communication to identify and prioritize plans of actions and steps at various thresholds of escalation surrounding a cyber incident;
- Improve the ability to gather, analyze, and de-conflict multiple sources of information to produce timely and actionable situational awareness;
- Issue alerts and warnings across a broad range of stakeholders to raise awareness and initiate incident response activities, consequence management, and business continuity plans;
- Reduce redundancy and duplication that could adversely impact effective coordination by articulating and affirming various roles and responsibilities;
- Enhance predictability and sustainability to improve collaboration necessary to manage consequences and assess and mitigate impact; and
- Include flexibility and agility to adapt to emerging events and activities.

Operational planning is conducted across the broader community and is an inherent responsibility of every level of government and the private sector. Operational plans should be routinely exercised to ensure identify gaps and establish continuous improvement plans to improve preparedness and effectiveness of the information sharing process surrounding a cyber incident.

This NCIRP is not an operational plan for responding to cyber incidents. However, it should serve as the primary strategic approach for stakeholders to utilize when developing agency- and organization-specific operational plans. This common doctrine will foster unity of effort for emergency operations planning and it will help those affected by cyber incidents to understand how federal departments, agencies, and other national-level broader community partners provide resources to support the SLTT communities and private sector response operations.

Response Operational Planning

Both the Comprehensive Preparedness Guide (CPG) 101⁴⁵ and the Response Federal Interagency Operational Plan (FIOP)⁴⁶ are foundational documents that agencies and organizations can leverage and tailor to cyber incidents to develop their own operational response plans.

⁴⁵ CPG 101, Developing and Maintain Emergency Operations Plans, Version 2. November 2010. <https://www.fema.gov/media-library/assets/documents/25975>

⁴⁶ Response Federal Interagency Operational Plan, Second Edition. August 2016. https://www.fema.gov/media-library-data/1471452095112-507e23ad4d85449ff131c2b025743101/Response_FIOP_2nd.pdf

The CPG 101 provides information on various types of plans and guidance on the fundamentals of planning. Federal plans for incidents are developed using a six-step process, in alignment with the steps described in CPG 101:

- Form a collaborative planning team
- Understand the situation
- Determine the goals and objectives
- Develop the plan
- Prepare, review, and approve the plan
- Implement and maintain the plan.

The Response FIOP outlines how the Federal Government delivers the response core capabilities. The Response FIOP provides information regarding roles and responsibilities, identifies the critical tasks an entity takes in executing core capabilities, and identifies resourcing and sourcing requirements. It addresses interdependencies and integration with the other mission areas throughout the plan's concept of operations. It also describes the management of concurrent actions and coordination points with the areas of prevention, protection, mitigation, and recovery. It does not contain detailed descriptions of specific department or agency functions, as such information is located in department- or agency-level operational plans.

The NRF and NIMS guide the Response FIOP. The NRF is based on the concept of tiered response, with an understanding that most incidents start at the local and tribal level, and as needs exceed resources and capabilities, additional SLTT and federal assets are applied. The Response FIOP, therefore, aligns with other SLTT, insular area, and federal plans to ensure that all response partners share a common operational focus. Similarly, integration occurs at the federal level among the departments, agencies, and nongovernmental partners that compose the respective mission area through the frameworks, FIOPs, and departmental and agency operations plans.

Application

While the NRF does not direct the actions of other response elements, the guidance contained in the NRF and the Response FIOP informs SLTT and insular area governments, as well as nongovernment organizations and the private sector, regarding how the Federal Government responds to incidents. These partners can use this information to inform their planning and ensure that assumptions regarding federal assistance and response, and the manner in which federal support will be provided, are accurate.

Developing an Internal Cyber Incident Response Plan

Public and private sector entities should consider creating an entity-specific operational cyber incident response plan to further organize and coordinate their efforts in response to cyber incidents. Each organization should consider a plan that meets its unique requirements and relates to the organization's mission, size, structure, and functions.

The National Institute of Standards and Technology Special Publication 800-61 (revision 2)⁴⁷ outlines several elements to consider when developing a cyber incident response plan. Each plan should be tailored and prioritized to meet the needs of the organization and adhere to current information sharing and reporting requirements, guidelines, and procedures, where they exist. As

⁴⁷ NIST SP 800-61 Revision 2, Computer Incident Handling Guide. August 2012.
<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>

appropriate, public and private sector entities are encouraged to collaborate in the development of cyber incident response plans to promote shared situational awareness, information sharing, and acknowledge sector, technical, and geographical interdependences.

The elements below serve as a starting point of important criteria to build upon for creating a cyber incident response plan:

- Mission
- Strategies and goals
- Organizational approach to incident response
- Risk assessments
- Cyber Incident Scoring System/Criteria⁴⁸
- Incident reporting and handling requirements
- How the incident response team will communicate with the rest of the organization and with other organizations
- Metrics for measuring the incident response capability and its effectiveness
- Roadmap for maturing the incident response capability
- How the program fits into the overall organization
- Communications with outside parties, such as:
 - Customers, constituents, and media
 - Software and support vendors
 - Law enforcement agencies
 - Incident responders
 - Internet service providers
 - Critical infrastructure sector partners
- Roles and responsibilities (preparation, response, recovery)
 - State Fusion Center
 - Emergency Operations Center
 - Local, regional, state, tribal, and territorial government
 - Private sector
 - Private citizens
- A training and exercise plan for coordinating resources with the community
- Plan maintenance schedule/process.

⁴⁸ The NCCIC Cyber Incident Scoring System could be used as a basis for an organizations operations center to assist in the internal elevation of a particular incident. <https://www.us-cert.gov/NCCIC-Cyber-Incident-Scoring-System>.

Annex H: Core Capability/NIST Cybersecurity Framework/PPD-41 Crosswalk

The NCIRP Crosswalk describes the relationship between the NIST Cybersecurity Framework and PPD-41. By walking through the table below, each core capability is cross-referenced to ensure continuity and connection between the three documents. This table should be leveraged as a starting point that may assist in the NCIRP's response activities under each core capability, understanding the NIST's functions and categories, and the PPD's respective Lines of Effort.

NCIRP Core	Core Capability	NIST Cybersecurity Framework Functions and Categories					Alignment to PPD-41 Lines of Effort
		Identify	Protect	Detect	Respond	Recover	
Access Control	Apply and support necessary physical, technological, and cyber measures to control admittance to critical locations and systems.		Access Control Protective Technology				Asset Response
Cybersecurity	Protect (and, if needed, restore) computer networks, electronic communications systems, information, and services from damage, unauthorized use, and exploitation.	Asset Management Business Environment Risk Assessment Risk Management Strategy	Access Control Data Security Information Protection Processes and Procedures Protective Technology	Anomalies and Events Security Continuous Monitoring Detection Processes	Communications Response Planning Analysis Mitigation	Communications Improvements Recovery Planning	Asset Response
Forensics and	Forensic investigations and efforts to provide attribution for an incident are complimentary functions that often occur in parallel during a significant cyber incident.				Analysis		Threat Response Asset Response Intelligence Support

NCIRP Core Capability	Core Capability Description	NIST Cybersecurity Framework Functions and Categories					Alignment to PPD-41 Lines of Effort
		Identify	Protect	Detect	Respond	Recover	
Infrastructure	Stabilize critical infrastructure functions, minimize health and safety threats, and efficiently respond and recover systems and services to support a viable, resilient community following malicious cyber activity.	Asset Management Business Environment Risk Assessment	Access Control Data Security Information Protection Processes and Procedures Protective Technology	Anomalies and Events Security Continuous Monitoring Detection Processes		Communications Improvements Recovery Planning	Asset Response
Intelligence and Information Sharing	Provide timely, accurate, and actionable information resulting from the planning, direction, collection, exploitation, processing, analysis, production, dissemination, evaluation, and feedback of available information concerning threats of malicious cyber activity to the United States, its people, property, or interests. Intelligence and information sharing is the ability to exchange intelligence, information, data, or knowledge among government or private sector entities, as appropriate.	Asset Management Business Environment	Awareness & Training Data Security	Security Continuous Monitoring Detection Processes	Communications Analysis Mitigation Improvements	Communications	Threat Response Asset Response Intelligence Support
Interdiction and Disruption	Delay, divert, intercept, halt, apprehend, or secure threats						Threat Response

NCIRP Core Capability	Core Capability Description	NIST Cybersecurity Framework Functions and Categories					Alignment to PPD-41 Lines of Effort
		Identify	Protect	Detect	Respond	Recover	
	related to malicious cyber activity.						
Logistics and Supply Chain Management	Facilitate and assist with delivery of essential commodities, equipment, and services to include the sustainment of responders in support of responses to systems and networks impacted by malicious cyber activity. Synchronize logistics capabilities and enable the restoration of impacted supply chains.	Business Environment					Asset Response
Operational Communications	Ensure the capacity for timely communications in support of security, situational awareness, and operations by any and all means available, among and between entities affected by the malicious cyber activity and all responders.	Asset Management		Communications	Communications		Threat Response Asset Response Intelligence Support
Operational Coordination	Establish and maintain a unified and coordinated operational structure and process that appropriately integrates all critical stakeholders and supports execution of core capabilities.	Governance Risk Assessment Risk Management	Anomalies and Events				Threat Response Asset Response Intelligence Support
Planning	Conduct a systematic process engaging the whole community, as appropriate, in the development of executable strategic,				Response Planning	Recovery Planning Improvements	Threat Response Asset Response

NCIRP Core Capability	Core Capability Description	NIST Cybersecurity Framework Functions and Categories					Alignment to PPD-41 Lines of Effort
		Identify	Protect	Detect	Respond	Recover	
	operational, and/or tactical-level approaches to meet defined objectives.						Intelligence Support
Public Information and Warning	Deliver coordinated, prompt, reliable, and actionable information to the whole community through the use of clear, consistent, accessible, and culturally and linguistically appropriate methods to effectively relay information regarding significant threat or malicious cyber activity, as well as the actions being taken and the assistance being made available, as appropriate.				Communications	Communications	Threat Response Asset Response Intelligence Support
Screening, Search and Detection	Identify, discover, or locate threats of malicious cyber activity through active and passive surveillance and search procedures.			Anomalies and Events Security Continuous Monitoring Detection Processes			Threat Response Asset Response Intelligence Support
Situational Assessment	Provide all decision makers with decision-relevant information regarding the nature and extent of the malicious cyber activity, any cascading effects, and the status of the response. In the context of a cyber	Business Environment Communications Awareness and Training		Detection Processes	Communications	Communications	Threat Response Asset Response Intelligence Support

NCIRP Core Capability	Core Capability Description	NIST Cybersecurity Framework Functions and Categories					Alignment to PPD-41 Lines of Effort
		Identify	Protect	Detect	Respond	Recover	
	incident, this capability focuses on rapidly processing and communicating large quantities of information from across the whole community from the field-level to the national-level to provide all decision makers with the most current and accurate information possible.						
Threats and Hazards Identification	Identify the threats of malicious cyber activity to networks and system; determine the frequency and magnitude; and incorporate this into analysis and planning processes so as to clearly understand the needs of an entity.			Anomalies and Events Security Continuous Monitoring Detection Processes			Threat Response

Annex I: Additional Resources

The following resources can be leveraged by both the private and public sector. Entities can use this list as a starting point for understanding cyber incident response, vulnerability updates, data breach information, risk management, and organizations that serve as a points of contacts for the public and private sector. This non exhaustive alphabetical list provides a wide range of information that can also be leveraged beyond the scope of this document.

- Center for Internet Security: www.cisecurity.org
- CIS Critical Controls: <https://www.cisecurity.org/critical-controls.cfm>
- Cyber Incident Severity Schema: <https://www.whitehouse.gov/sites/whitehouse.gov/files/documents/Cyber+Incident+Severity+Schema.pdf>
- DHS Critical Infrastructure Cyber Community Voluntary Program: <https://www.us-cert.gov/ccubedvp>
- Government Coordinating Councils: <https://www.dhs.gov/gcc>
- Information Sharing and Analysis Organizations: <https://www.isao.org/>
- Infragard: www.infragard.org
- Industrial Control System Security Computer Emergency Response Team: <https://ics-cert.us-cert.gov>
- Malware Investigator: <https://www.malwareinvestigator.gov/>
- MITRE Common Vulnerabilities and Exposures: <https://cve.mitre.org/>
- Multi-State Information Sharing and Analysis Center: <https://msisac.cisecurity.org/>
- National Council of Information Sharing and Analysis Centers: <http://www.nationalisacs.org/>
- National Incident Management System: <https://www.fema.gov/national-incident-management-system>
- National Vulnerability Database: <https://nvd.nist.gov/>
- NIST Framework for Improving Critical Infrastructure Cybersecurity: <https://www.nist.gov/cyberframework>
- NIST National Checklist Program Repository: <https://web.nvd.nist.gov/view/ncp/repository>
- NIST SP 800-61:: Revision 2: Computer Incident Handling Guide: <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>:
- NIST SP 800-37: Guide to Applying the Risk Management Framework to Federal Information Systems: <http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf>
- NVD Common Vulnerability Scoring System: <https://nvd.nist.gov/cvss.cfm> Sector Coordinating Councils: <https://www.dhs.gov/scc>
- US-CERT Website: www.us-cert.gov

Annex J: Acronym List

CRG	Cyber Response Group
CTIIC	(Office of the Director of National Intelligence) Cyber Threat Intelligence Integration Center
DC3	Department of Defense Cyber Crime Center
DHS	Department of Homeland Security
DOC	Department of Commerce
DoD	Department of Defense
DOE	Department of Energy
DoDIN	Department of Defense Information Network
DOJ	Department of Justice
DOS	Department of State
ESF	Emergency Support Functions
FBI	(Department of Justice) Federal Bureau of Investigations
FEMA	(Department of Homeland Security) Federal Emergency Management Agency
GCC	Government Coordinating Council
HSI	(Department of Homeland Security) Homeland Security Investigations
IC	Intelligence Community
IC3	Internet Crime Complaint Center
IC-SCC	Intelligence Community Security Coordination Center
ICE	(Department of Homeland Security) Immigrations and Customs Enforcement
ICT	Information and Communications Technology
INTERPOL	International Criminal Police Organization
ISAC	Information Sharing and Analysis Center
ISAO	Information Sharing and Analysis Organization
JOC	Joint Operations Center
MS-ISAC	Multi-State Information Sharing and Analysis Center
NCIRP	National Cyber Incident Response Plan
NCCIC	(Department of Homeland Security) National Cybersecurity and Communications Integration Center
NCIJTF	(Federal Bureau of Investigations) National Cyber Investigative Joint Task Force
NCPA	National Cybersecurity Protection Act
NCTOC	National Security Agency Cybersecurity Threat Operations Center
NIMS	National Incident Management System
NIST	National Institute of Standards and Technology

NIPP	National Infrastructure Protection Plan
NRF	National Response Framework
ODNI	Office of the Director of National Intelligence
PII	Personally Identifiable Information
PPD	Presidential Policy Directive
SCC	Sector Coordinating Council
SLTT	State, Local, Tribal, and Territorial
SLTT GCC	State, Local, Tribal, and Territorial Government Coordinating Council
SSA	Sector Specific Agency
UCG	Unified Coordination Group
US-CERT	United States – Computer Emergency Readiness Team
USCYBERCOM	(Department of Defense) United States Cyber Command



Homeland
Security



Information Technology

Critical Infrastructure and Key Resources
Sector-Specific Plan as input to the
National Infrastructure Protection Plan

May 2007



Homeland
Security

Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE MAY 2007		2. REPORT TYPE		3. DATES COVERED 00-00-2007 to 00-00-2007	
4. TITLE AND SUBTITLE Information Technology: Critical Infrastructure and Key Resources Sector-Specific Plan as Input to the National Infrastructure Protection Plan				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Homeland Security, Washington, DC, 20528				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT Same as Report (SAR)	18. NUMBER OF PAGES 108	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			



Information Technology Sector Government Coordinating Council Letter of Concurrence

The National Infrastructure Protection Plan (NIPP) provides the unifying structure for the integration of critical infrastructures and key resources (CI/KR) protection efforts into a single national program. The NIPP provides an overall framework for integrating programs and activities that are underway in the various sectors, as well as new and developing CI/KR protection efforts. The NIPP includes 17 sector-specific plans (SSPs) that detail the application of the overall risk management framework to each specific sector.

Each SSP describes a collaborative effort between the private sector; State, local, and tribal governments; nongovernmental organizations; and the Federal Government. This collaboration will result in the prioritization of protection initiatives and investments within and across sectors to ensure that resources can be applied where they contribute the most to risk mitigation by lowering vulnerabilities, deterring threats, and minimizing the consequences of attacks and other incidents.

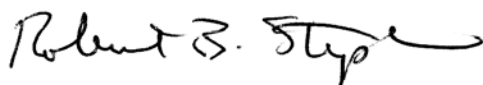
Over the past year, the Department of Homeland Security (DHS) worked closely with members of the Information Technology (IT) Government Coordinating Council (GCC), including representatives from the Departments of Commerce, Defense, Justice, State, and Treasury, the Office of the Director of National Intelligence, the Office of Management and Budget, and the National Association of State Chief Information Officers, to develop the IT SSP in partnership with the IT Sector Coordinating Council (SCC). GCC members contributed time and expertise to develop and finalize the IT SSP and will:

- Support the concepts and processes outlined in the IT SSP to carry out their assigned functional responsibilities regarding the protection of CI/KR as described herein;
- Work with DHS, as appropriate and consistent with their own agency-specific authorities, resources, and programs, to implement programs that enhance CI/KR protection;
- Cooperate and coordinate with DHS, in accordance with guidance provided in Homeland Security Presidential Directive 7, as appropriate and consistent with their own agency-specific authorities, resources, and programs, to facilitate CI/KR protection;

- Develop or modify existing interagency and agency-specific CI/KR plans, as appropriate, to incorporate concepts and actions outlined in the IT SSP; and
- Develop and maintain partnerships for CI/KR protection with appropriate State, regional, local, tribal, and international entities; the private sector; and nongovernmental organizations.

DHS looks forward to continuing to work in partnership with IT GCC and IT SCC representatives and other Sector security partners on the implementation of the IT SSP.

Sincerely,



Robert B. Stephan
Assistant Secretary for
Infrastructure Protection
National Protection and Programs Directorate
Department of Homeland Security
Co-Chair, IT GCC



Gregory Garcia
Assistant Secretary for Cyber Security
and Communications
National Protection and Programs Directorate
Department of Homeland Security
Co-Chair, IT GCC

December 29, 2006

The Honorable Robert B. Stephan
Assistant Secretary for Infrastructure Protection
U.S. Department of Homeland Security
Washington, D.C. 20528

Subject: Letter of Coordination, Information Technology Sector Specific Plan



Dear Mr. Assistant Secretary:

The members of the Information Technology (IT) sector, organized through our Sector Coordinating Council, the IT-SCC, share a commitment to improving America's homeland security through our stewardship of critical technology infrastructures. Furthering our public-private partnership with the Department under the framework of the National Infrastructure Protection Plan (NIPP), in 2006, members of the IT-SCC voluntarily organized to work with the government to develop an IT-Sector Specific Plan (SSP). IT-SCC members committed substantial resources, and working together with DHS' National Cyber Security Division (NCSD), we developed a plan document that details improvements that will enhance national capabilities for (1) prevention and protection through risk management, (2) situational awareness, and (3) response, recovery and reconstitution of America's information technology infrastructure. The resulting plan represents the most comprehensive joint planning effort undertaken by IT-Sector public-private security partners.

Having built consensus for the key elements of the plan, the IT-SCC believes that the document's goals and objectives—while ambitious—chart a course for long-term collaboration with the Federal government, including the Department of Homeland Security. The IT-SSP identifies important specific opportunities for collaborative efforts between and among the private sector, State, local and tribal governments, nongovernmental organizations, and the Federal Government. By working together, private and public IT-sector security partners can prioritize protective initiatives and investments within and across sectors. Such collaboration can ensure that limited government resources are applied effectively and efficiently. Over time this will mitigate risks by reducing vulnerabilities, deterring threats, and minimizing the consequences of incidents. Creating a value proposition for both government and private sector participation in this process is critical to fostering increased resilience across shared infrastructures and the supply chains that enable critical IT Sector functions.

Achieving the goals and objectives of the SSP will present some challenges for both public and private security partners. For example, determining, identifying, and obtaining the necessary resources required to perform national level risk assessments of critical IT sectors functions, enhance incident response programs, or develop new programs to support recovery and reconstitution will require working closely with Congress, to prioritize DHS programs (or eliminating unnecessary programs) to meet the agreed upon objectives of the SSP. Similarly, private enterprises will work to develop business cases to make investments of time and resources of their own in support of SSP objectives.

Of particular importance to our sector and this Plan in relation to the companion documents developed by our peer Critical Infrastructure sectors is our approach to the identification of sector facilities in the National Asset Database (NADB). IT-SCC members appreciate DHS' recognition that the unique and virtual nature of critical IT-sector functions do not translate easily into NADB entries. The criticality of sector functions is situational and dependent on their utilization. Accordingly, the sector is generally focused on a threat-scenario-driven risk assessment approach to ascertaining IT Sector Critical Functions and sub-functions, rather than simply cataloging specific or generic assets owned or operated by individual sector members. Any information entered into the NADB should reflect this industry-led, top-down risk assessment approach based on the identified Sector Critical Functions, and be based upon the decision of individual industry owners and operators acting in cooperation with the Department and other agencies. Through the implementation of the IT SSP risk management process, the IT Sector will work with DHS to understand and protect systems, networks, and functions which have unique characteristics or play essential roles in ensuring national and economic security and public health, safety, and confidence.

The members of the IT community, represented by the IT-SCC, will continue to work with DHS, its other government partners (federal, state, local, and tribal) and other security partners to develop and implement the recommendations embodied in this initial iteration of the IT-SSP. It is hoped that this collaboration will result in assessments of risk to IT architectures and functions in a way that will help better prioritize protection initiatives and investments within the sector. The members of the IT-SCC, while sharing the goals expressed in the plan, recognize that by our sector's consensus participation in the NIPP/SSP process, no specific commitment of individual action can be made.

Thank you for your continued support of the IT Sector as we mobilize our constituencies around critical infrastructure protection. We look forward to working in this partnership and to future interaction with the other Sector Coordinating Councils both bilaterally and via the Partnership for Critical Infrastructure Security.

Sincerely,
Information Technology Sector Coordinating Council



Guy Copeland
Chairperson



Michael Aisenberg
Vice Chairperson

cc: The Honorable Gregory T. Garcia, Assistant Secretary for Cyber Security & Telecommunications,
U.S. Department of Homeland Security

Members of the IT-SCC Executive Committee:

Guy Copeland, Computer Sciences Corporation, Chairperson
Michael Aisenberg, VeriSign, Vice Chairperson
Larry Clinton, Internet Security Alliance (ISA), Treasurer
Robert B. Dix, Jr., Juniper Networks, Inc., Acting Secretary
David Barron, BellSouth
Ken Watson, Cisco Systems, Inc.
Phil Reiting, Microsoft Corporation
(Vacant), Unisys Corporation
Howard A. Schmidt, R & H Security Consulting LLC
Jerry Cochran, Information Systems Security Association (ISSA)
Liesyl Franz, Information Technology Association of America (ITAA)
James Bean, Verizon, Communications SCC Liaison

Designated Representatives of the IT-SCC Members:

Bell Security Solutions Inc.	Electronic Industries Alliance (EIA)	International Security Trust
BellSouth Corporation	Entrust, Inc.	and Privacy Alliance (ISTPA)
CA, Inc	IBM Corporation	KPMG LLP
Center for Internet Security	Information Systems Security	Lockheed Martin
Cisco Systems, Inc.	Association (ISSA)	McAfee, Inc.
Computer and Communications	Information Technology Association	Microsoft Corporation
Industry Association	of America (ITAA)	NTT America
Computer Sciences Corporation	Intel Corporation	R & H Security Consulting LLC
Cyber Security Industry Alliance	Information Technology - Information	Seagate Technology
(CSIA)	Sharing & Analysis Center (IT-ISAC)	Symantec Corporation
Computing Technology Industry	International Systems Security	U.S. Internet Service Provider
Association	Engineering Association (ISSEA)	Association (USISPA)
EWA Information & Infrastructure	Internet Security Alliance (ISA)	Unisys Corporation
Technologies, Inc.		VeriSign



Table of Contents

Executive Summary	1
Sector Background and Goals	2
Risk Management	2
Develop and Implement Protective Programs	3
Information Sharing	3
CI/KR Protection Research and Development	4
Managing and Coordinating Sector Responsibilities	4
Implementing the SSP and Tracking Progress	4
Introduction and Purpose	5
Document Organization	7
1. Sector Profile and Goals	9
1.1 Definition	9
1.2 Scope	10
1.3 Sector Security Goals and Objectives	11
1.4 Partnering for Security	12
1.5 Authorities	15
1.6 Actions	15
1.6.1 Near Term (~1 year)	15
1.6.2 Long Term (1-3 years)	16
2. Risk Management	17
2.1 Background of the IT Sector's Risk Environment	18
2.1.1 Various Entities' Risk Management Approaches	18
2.2 Developing an IT Sector Risk Profile	19
2.2.1 National IT Sector Risk Management Approach	20
2.3 Identifying Critical Functions	20
2.3.1 Screening and Assessing Consequences	20
2.3.2 Decomposing Critical IT Sector Functions	22
2.4 Assessing Threats, Vulnerabilities, Consequences, and Mitigations	22
2.4.1 Analyzing Threats	22
2.4.2 Assessing Vulnerabilities	23

2.4.3	Evaluating Consequences	24
2.4.4	Identifying Mitigations	24
2.5	Prioritizing for the IT Sector Risk Profile	25
2.6	Risk Management Information	26
2.7	Actions	27
2.7.1	Near Term (~1 year)	27
2.7.2	Long Term (1-3 years)	28
3.	Develop and Implement Protective Programs	29
3.1	Current IT Sector Protective Programs	29
3.2	Identification and Implementation of New Protective Programs	31
3.2.1	Establish a Protective Program Working Group	31
3.2.2	Determine Needs and Capabilities	31
3.2.3	Identify Protective Actions	32
3.2.4	Develop an Implementation Plan	32
3.3	Protective Program Performance	32
3.4	Actions	33
3.4.1	Near Term (~1 year)	33
3.4.2	Long Term (1-3 years)	33
4.	Information Sharing	35
4.1	Types of Information	35
4.2	Information Originators and Users	37
4.3	An Enhanced IT Sector Information Sharing Framework	39
4.3.1	Information Sharing Focal Points	40
4.3.2	Policies and Procedures for Sharing and Reporting Incidents	41
4.3.3	Procedures for Protecting and Disseminating Sensitive Proprietary Industry Information	41
4.3.4	Access to Classified and Sensitive But Unclassified (SBU) Government Information	42
4.3.5	Mechanisms for Communicating and Disseminating Information	43
4.4	Actions	43
4.4.1	Near Term (~1 year)	43
4.4.2	Long Term (1-3 years)	45
5.	CI/KR Protection Research and Development	47
5.1	Current IT Sector Research and Development	47
5.2	IT Sector R&D Priorities	48
5.3	Coordinating IT Sector R&D Priorities	49
5.4	Actions	51
5.4.1	Near Term (~1 year)	51

5.4.2 Long Term (1-3 years)	51
6. Managing and Coordinating Sector Responsibilities	53
6.1 Program Management Approach	53
6.2 Processes and Responsibilities	53
6.2.1 SSP Maintenance and Update	53
6.2.2 Annual Reporting	53
6.2.3 Resources and Budgets	54
6.2.4 Training and Education	54
6.3 Roles and Responsibilities	56
6.3.1 Sector-Specific Agency	56
6.3.2 IT Sector Coordinating Council	57
6.3.3 IT Government Coordinating Council	57
6.3.4 Shared Cross-Sector Cyber Security Responsibilities	58
6.4 Actions	58
6.4.1 Near Term (~1 year)	58
6.4.2 Long Term (1-3 years)	58
7. Implementing the SSP and Tracking Progress	59
7.1 Tracking Progress Challenges	59
7.2 Measurement Overview	59
7.3 Measurement Approach	60
7.4 Goals and Objectives Measurement	60
7.5 Activities Implementation	62
7.6 Reporting on Progress	63
7.7 Actions	64
7.7.1 Near Term (~1 year)	64
7.7.2 Long Term (1-3 years)	64
Appendix 1: List of Acronyms and Abbreviations	65
Appendix 2: Authorities	69
Homeland Security/National Security IT Authorities	69
National Strategies	71
Management and Acquisition of Federal Government Information Technology	72
Information Technology Audit-Related Authorities	73
National Preparedness and Response Authorities Related to Information Technology	74
Information Technology Communications Related Authorities	74
Information Technology Privacy Authorities and Information Protection Related Authorities	74
International Standards and Guidelines	75

Appendix 3: Common Risk Management Frameworks	77
Appendix 4: IT Sector-Related Protective Programs	79
Appendix 5: Action Items	89

List of Figures

Figure 2-1. Developing the IT Sector Risk Profile	19
Figure 2-2. Notional Risk Priority Matrix	25
Figure 2-3. Risk Management Information	26
Figure 4-1. Information Flows	37
Figure 4-2. Notional Relationship Among Security Partners and Types of Information	39
Figure 7-1. IT Sector Measurement Approach	60
Figure 7-2. Notional Gantt Chart to Indicate Goal and Objective Implementation Progress at Q4 2008	61
Figure 7-4. Notional Gantt Chart to Indicate Activity Implementation Progress at Q4 2008	63

List of Tables

Table 1-1. Examples of IT Security Partners	14
Table 2-1. Critical IT Sector Functions and Descriptions	21
Table 3-1. Protective Program Capabilities that Support IT Sector Goals	30
Table 4-1. Types of Information Produced by Security Partners (Notional Template)	38
Table A4-1. Existing Protective Programs that Support the Overarching IT Sector Goals	79

Executive Summary

Information technology (IT) is central to our Nation's security, economy, and public health and safety. Businesses, governments, academia, and private citizens are increasingly dependent on IT Sector functions and services as are all other critical infrastructure sectors' products and services. The Sector has diverse global operations that are interdependent and interconnected with those of other infrastructure sectors. These operations face numerous, multifaceted, global threats every day. Individual IT Sector entities proactively manage risk to their own operations and those of their customers,¹ through constant monitoring and mitigation activities designed to prevent daily incidents from becoming significant disruptions to national security, the economy, and public health and safety. Although the IT infrastructure has a certain level of inherent resilience, its interdependent and interconnected structure presents challenges and opportunities for coordinating public and private sector preparedness activities.

Daily protective activities by individual sector entities to prevent, protect against, and mitigate threats and disruptions contribute to the sector's overall steady state of preparedness. This plan focuses on public and private sector planning to enhance the ability of the sector as a whole to prevent, protect against, mitigate, and respond to nationally significant events, technological emergencies, and Presidentially-declared disasters that threaten, disrupt, or cripple IT Sector infrastructure.

Various efforts championed by the public and private sectors have been undertaken to address infrastructure protection and cyber security. The Homeland Security Act of 2002 required the first-ever all-encompassing coordinated national critical infrastructure and key resources (CI/KR) protection effort. Homeland Security Presidential Directive 7 (HSPD-7) identifies 17 CI/KR sectors, including the IT Sector, and requires Federal agencies, coordinated by the Department of Homeland Security (DHS), to identify, prioritize, and coordinate the protection of the Nation's critical infrastructure. The National Infrastructure Protection Plan (NIPP) and its complementary Sector-Specific Plans (SSP) provide a consistent, unifying structure for integrating existing and future CI/KR protection efforts. They also provide the core processes and mechanisms to enable government and private sector security partners to work together to implement CI/KR protection initiatives.

Public and private sector security partners have an enduring interest in assuring the availability of the infrastructure and promoting its resilience. The IT SSP represents an unprecedented partnership and collaboration between the IT public and private sectors to address the complex challenges of CI/KR protection. Public and private sector organizations each represent and bring unique capabilities to the partnership, and derive value from the exchange. Successful CI/KR protection is the commitment of IT Sector public and private sector security partners to share information and provide the tools and capabilities necessary for an effective partnership.

¹ As determined by contracts with those customers

The IT SSP was collaboratively developed by DHS' National Cyber Security Division (NCSD) as the Sector Specific Agency (SSA) for the IT Sector and sector security partners, including the IT Sector Coordinating Council (SCC) and IT Government Coordinating Council (GCC). The IT SSP is a planning document that provides guidance on how public and private partners will work together to protect IT Sector CI/KR. It does not provide specific procedures for individual Sector entities' operations and is not designed to guide Federal or State government efforts to respond to events. For the purposes of the IT SSP, "response" refers to individual entity activities as well as joint public and private sector activities, to position the Sector to ensure that any disruptions or manipulations of the IT infrastructure are brief, infrequent, manageable, geographically isolated, and minimally detrimental to the welfare of the United States. Federally coordinated response, including activities addressed by the National Response Plan, will be specifically referenced as such. Although this document is the first jointly developed IT SSP, it will not be the last. Threats and vulnerabilities are continually evolving, and consequently plans and programs for addressing these must evolve accordingly.

Sector Background and Goals

The IT Sector is composed primarily of virtual and distributed functions necessary to provide IT products and services. These critical IT Sector functions are provided by a combination of entities—often owners and operators and their respective associations—that provide hardware, software, IT systems, and services. These entities maintain and reconstitute the network, including the Internet. The Internet encompasses the global infrastructure of packet-based networks and databases that use a common set of protocols to communicate. The networks are connected by various transports, and the availability of these networks and services is the collective responsibility of the IT and Communications Sectors.

The IT SSP provides a framework for identifying and managing Sector risk during the steady-state (i.e., routine day-to-day business operations) to prevent, protect against, mitigate, and prepare for nationally significant events, including those cyber or physical events, technological emergencies, or Presidentially-declared disasters, that threaten, disrupt, or cripple the IT Sector infrastructure. Public and private sector security partners have collaborated to identify overarching goals for the sector that are intended to ensure overall Sector preparedness. Pursuit of these goals requires individual actions by a wide array of public and private security partners.

IT Sector Goals

- Prevention and Protection Through Risk Management
- Situational Awareness
- Response, Recovery, and Reconstitution

Risk Management

Public and private sectors are collaborating to address risks that could affect the ability of the Sector's critical functions to support the economy and national security. Given the IT Sector's complex and global operations and the diverse and interconnected nature of its supporting infrastructure, the Sector is using a qualitative, top-down approach that considers the Sector security goals and objectives and then identifies critical Sector functions. The resulting sector-wide risk approach described in the IT SSP addresses the three factors of risk as described in the NIPP—threat, vulnerability, and consequence—and focuses on those IT functions with national consequence. Many enti-

IT Sector Critical Functions

- Provide IT Products and Services
- Provide Incident Management Capabilities
- Provide Domain Name Resolution Services
- Provide Identity Management and Associated Trust Support Services
- Provide Internet Based Content, Information, and Communications Services
- Provide Internet Routing, Access and Connection Services

ties have robust risk management activities in place. As such, the IT SSP does not provide guidance for individual entities' risk management activities. Coordination of risk management activities by IT Sector security partners should help focus efforts and resources on ensuring the continued availability of critical IT Sector functions, products, and services and improved resilience of the nationally critical IT infrastructure.

The IT Sector approach to risk assessment consists of three steps: (1) identifying critical functions; (2) assessing threats, vulnerabilities, consequences, and mitigations; and (3) assessing and prioritizing risks. Critical IT Sector functions are identified and evaluated using consequences to focus on only those that meet certain thresholds for national significance. By defining critical IT Sector functions during development of the IT SSP, the IT Sector has completed the first step of the risk assessment approach.² The IT Sector will then apply threats to their critical functions to identify vulnerabilities. An all-hazards approach that addresses the spectrum of natural and manmade threats will be used. The IT Sector will complement the traditional threat assessment approach with additional factors based on capabilities and intent independent of known actors to consider emerging non-traditional threats. Vulnerabilities for critical functions and their applicable specific threat scenarios will be identified and assessed, along with mitigations that reduce specific risk factors.

Using HSPD-7 consequence categories and criteria for evaluating nationally significant events, the IT Sector's approach to consequence assessment identifies impacts on national and economic security and public health, safety, and confidence resulting from the disruption or degradation of a critical function. Consistent measurements will be used to evaluate threat, vulnerability, and consequence and enable the comparison of risks across the sector. The outcome of the national IT Sector risk assessment will be a prioritization of sector risks according to consequence and likelihood. The IT Sector will focus primarily on risks with high consequence and high likelihood.

Develop and Implement Protective Programs

Protective programs include measures or activities that are undertaken by various security partners to prepare for, prevent, protect, respond to, and recover from incidents that have the potential to impact critical IT Sector functions. Current protective programs provide capabilities for reducing vulnerabilities, analyzing threat, sharing information, and managing and responding to incidents. During the initial SSP development process, IT SCC and IT GCC members identified existing protective programs and areas where new programs or enhanced capabilities are needed, including robust coordinated response capabilities; reconstitution of data, communication services, and networks; out-of-band data delivery capability; and cyber grants for State governments.

The IT Sector will determine additional protective program needs identified through the risk management process. This process will be used to address those needs in which no viable private sector solution exists for meeting the need or high transaction costs or legal barriers would cause significant coordination and/or implementation challenges.

Information Sharing

Information sharing is a key element to fulfilling the overarching goals of the IT Sector and implementing the NIPP framework. Information sharing enables owners and operators, decision makers, managers, and others to detect, deter, and prevent attacks and incidents; identify trends; assess risks; provide warnings to help mitigate impacts; and coordinate response activities. IT Sector public and private sector security partners are focused on building and maintaining trusted relationships based on the simple premise that, for information to be useful, it must be shared with the right people at the right time. The IT Sector's approach focuses on sharing information between and among the government and those individuals who operate, administer, and own the IT infrastructure.

² These are public and private sector consensus critical IT Sector functions for Government Fiscal Year 2007. Annual planning enables the review and update of these functions to reflect changes in the IT Sector environment.

The IT Sector envisions an enhanced information sharing framework that identifies key focal points for policy and operational information sharing, processes, and procedures, and ways to facilitate access to information. The IT Sector’s vision for an ideal or future state of information sharing includes policy, cultural, organizational, and technological conditions that facilitate two-way, decentralized, yet coordinated information sharing.

CI/KR Protection Research and Development

In recent years, numerous committees and organizations have analyzed and reported on IT Sector security gaps. The result is a substantial body of work describing these gaps and proposing research and development (R&D) priorities to bridge them. The IT Sector leveraged this work to identify IT Sector R&D priorities based on the common themes established by prior analyses.

Addressing R&D priorities requires engaging multiple partners to pool resources to raise awareness and increase coordination. Establishment of an online clearinghouse for exchanging information and collaborating on IT Sector R&D priorities and conducting an annual IT Sector R&D workshop may provide mechanisms for outreach, review of research projects, consideration of gaps in the execution of national research priorities, and reaching consensus on general government and private sector requirements. In addition, a common taxonomy for exchanging information on progress toward accomplishing the sector’s goals for each R&D priority can promote understanding across the IT Sector and further collaboration.

IT Sector R&D Priorities

- Cyber Situational Awareness and Response
- Forensics
- Identity Management: Authentication, Authorization, and Accounting
- Intrinsic Infrastructure Protocols Security
- Modeling and Testing
- Control Systems Security
- Scalable and “Composable” Secure Systems
- Secure Coding, Software Engineering, and Hardware Design Improvement
- Trust and Privacy

Managing and Coordinating Sector Responsibilities

As described in HSPD-7, the DHS is responsible for managing and coordinating IT Sector CI/KR protection activities, including leading the development of an SSP for the IT Sector. Within the department, this responsibility has been delegated to NCSD. Sector responsibilities include maintenance and update of the SSP, annual reporting, resources and budgets, and training and education. Public and private sector security partners have common and unique roles and responsibilities.

Implementing the SSP and Tracking Progress

Tracking the progress of implementing the actions set forth in this plan is essential to the SSP’s success. A collaborative and iterative process that benefits from the voluntary input of the IT SCC and IT GCC members can track the SSP’s implementation most accurately and provide public and private sector security partners with a shared understanding of progress toward achieving the sector’s goals.

Implementing and tracking the action items in support of the sector’s goals and objectives requires commitment and resources (e.g., financial, time, personnel, and expertise) from the public and private sectors. Public and private sector security partners will need to prioritize the actions in this plan and proceed with implementation and tracking using an iterative approach while taking into account resource availability.

Introduction and Purpose

Information technology (IT) is central to our Nation's security, economy, public health, and safety. The IT Sector accounts for about 7 percent of the U.S. gross domestic product.³ On a daily basis, more than \$3 trillion worth of economic activity (e.g., securities sales settlements, check clearances, and interbank transfers) passes over secure Federal financial networks.⁴ IT systems enable this economic activity, which is essential to maintaining homeland and national security. Critical infrastructure and key resources (CI/KR) sectors rely on the IT Sector for products and services, including the reliable operation of networks and systems and the movement and storage of critical data. Conversely, the IT Sector relies on many other sectors, including the Energy and Communications Sectors, for daily operations.

The Sector has diverse global operations that are interdependent and interconnected with those of other infrastructure sectors. These operations face numerous multifaceted global threats daily. Individual IT Sector entities proactively manage risk to their own operations and those of their customers,⁵ through constant monitoring and mitigation activities designed to prevent daily incidents from becoming significant disruptions to national security, the economy, and public health and safety. Although the IT infrastructure has a certain level of inherent resilience, its interdependent and interconnected structure presents challenges and opportunities for coordinating public and private sector preparedness activities.

Since the 1990s, the public and private sectors have been working to address these challenges and opportunities. In 1997, a Presidential Commission identified the risks to critical infrastructures in a seminal public report, *Critical Foundations: Protecting America's Infrastructures*. Year 2000 initiatives and Executive Order 13231⁶ also made cyber security a priority, subsequently increasing funds available to secure Federal networks. Following the terrorist attacks of September 11, 2001, the Homeland Security Act of 2002 required the first comprehensive coordinated national CI/KR protection effort. The President's National Strategy to Secure Cyberspace articulates five national priorities for protecting against a debilitating disruption of the operation of information systems as part of national CI/KR protection efforts. In 2003, President George W. Bush issued Homeland Security Presidential Directive 7 (HSPD-7) requiring Federal agencies, coordinated by the Department of Homeland Security (DHS), to identify, prioritize, and coordinate the protection of CI/KR for the purposes of preventing, deterring, and mitigating the effects of deliberate efforts to destroy, incapacitate, or exploit them. Implementing this policy requires substantial commitment to public-private partnership. The directive identifies 17 CI/KR, including the IT Sector, and pairs each CI/KR sector with a sector-specific agency (SSA) for partnering on protective initiatives. HSPD-7 requires DHS to develop an overall National Infrastructure Protection Plan (NIPP) and specifically assigns DHS the mission of establishing uniform policies, approaches,

³ World Information Technology and Services Alliance, *Digital Planet 2006: The Global Information Economy*, May 2006, www.witsa.org/digitalplanet/2006/DP2006_ExecSummary.pdf.

⁴ Federal Reserve Board, "Telling the Fed's Story through Money in Motion," www.phil.frb.org/publicaffairs/pubs/ar03telling.pdf.

⁵ As determined by contracts with those customers.

⁶ Executive Order 13231, *Critical Infrastructure Protection in the Information Age*, October 2001.

guidelines, and methodologies for integrating infrastructure protection and risk management activities within and across sectors, along with developing metrics and criteria for related programs and activities.

The NIPP and its complementary Sector-Specific Plans (SSP) provide a consistent, unifying structure for integrating existing and future CI/KR protection efforts. They also define the core processes and mechanisms for public and private sector security partners⁷ to implement coordinated CI/KR protection initiatives. Implementation of the NIPP, its complementary SSPs, the National Response Plan (NRP), and the National Incident Management System (NIMS) define readiness targets, priorities, standards for assessment, strategies, and a system for assessing the Nation's overall preparedness across four mission areas: prevention, protection, response, and recovery.

Public and private sector security partners have an enduring interest in assuring the availability of the infrastructure. The IT Sector's market-based environment enables rapid innovation and drives investments in security to meet customers' changing needs and promote the resilience of the IT Sector. Prevention and protection through risk management, situational awareness, and response, recovery, and reconstitution efforts are most effective when full participation of public and private sector security partners exists; such efforts suffer without the full participation of either partner.

The IT SSP represents an unprecedented partnership and collaboration between the IT public and private sectors as they leverage their unique capabilities to address the complex challenges of CI/KR protection. The IT Sector entities involved in development of the SSP believe that its implementation will provide value for the sector and customers who rely on its products and services. As such, IT Sector entities involved in development of the SSP will work to convey the national security and business value for participation in SSP implementation activities to other members of the IT Sector.

IT private sector entities have a comprehensive understanding of critical IT Sector functions, capabilities, and infrastructure. This understanding enables the private sector to leverage existing information sharing mechanisms and its insights into risk mitigation and best practices to improve the Sector's security posture in a reasonable, feasible, and practical manner. Private sector entities manage risk to their business operations, voluntarily implement protective initiatives designed to enhance their steady-state physical, human, and cyber security, and manage response to day-to-day incidents to prevent and prepare for significant events. Individual private sector capabilities are also essential for incident management, as well as response, recovery, and reconstitution of essential government functions. Because the private sector can quickly focus on requirements and needs, it often takes the lead in developing and deploying innovative solutions, increasing the skills and availability of security professionals, and developing products and services that are responsive to the rapidly changing threat environment.

Federal Government coordination and leadership of IT Sector CI/KR protection efforts is justified and, in certain instances, required. For example, continuity of government (Federal, State, and local) requires ensuring the security and availability of governments' cyber and physical infrastructure necessary to support their essential missions and services. To fully leverage the unique capabilities of the private sector, the Federal Government is working to ensure that the private sector is engaged, as early as possible, in the development, implementation, and maintenance of initiatives and policies regarding ownership and operation of the private sector's products, services, and systems. In addition, government has a role to play in instances where high transaction costs or legal barriers lead to significant coordination problems, where government operations exist in the absence of private sector forces, or where critical shared resources are under provisioned. The public sector can create a legal and regulatory environment that stimulates and facilitates voluntary private sector efforts to improve security, including establishing the policies and protocol needed to share timely analytical and useable information about threats to the IT Sector. Finally, the public sector sponsors efforts such as cross-sector interdependency studies, research and development (R&D) into the security of basic Internet protocols, and research studies on return on investment (ROI) for businesses that undertake risk management efforts and implement improved security processes and tools.

⁷ The term "security partners" refers to the stakeholders in the NIPP planning process. These stakeholders include all government levels (Federal, State, Territorial, regional, local, and tribal), regional organizations, international partners, and private sector owners and operators.

Information sharing among and between public and private sector security partners is essential for achieving security. Through improved information sharing and analysis, the public and private sectors will be better equipped to identify threats and vulnerabilities, and to exchange mitigating and preventive tactics and resources to address them. Successful CI/KR protection requires the commitment of public and private IT Sector security partners to provide tools and capabilities for an effective partnership. Only with robust exchanges and rigorous critique and evolution of the sector's goals and priorities will the value proposition continue to be realized.

The IT SSP was developed collaboratively by IT Sector security partners, including representatives from the DHS's National Cyber Security Division (NCSD), the IT Sector Coordinating Council (SCC), and the IT Government Coordinating Council (GCC). The SSP is a planning document that focuses on meeting sector goals that are most pressing for homeland, economic, and national security purposes and identifies actions (current, near term, and long term) for steady-state preparedness, including prevention and protection of critical IT Sector functions that enable sector response and recovery activities. The SSP does not provide specific procedures for individual IT Sector entities' operations. The SSP:

- Outlines the IT Sector security partners' joint implementation of the NIPP risk management framework by describing an approach for identifying, assessing, prioritizing, and protecting critical IT Sector functions;
- Establishes shared IT Sector goals and objectives and aligns initiatives to meet them;
- Describes roles, responsibilities, and opportunities that NCSD, IT SCC, IT GCC, and other security partners can play in implementing the SSP; and
- Provides opportunities for integrating public and private sector preparedness efforts with tools and technologies essential for effective incident response, system remediation, and reconstitution under the NRP and NIMS.

Although this document is the first jointly developed IT SSP, it will not be the last. Threats and vulnerabilities evolve continually, and consequently plans and programs for addressing them must evolve accordingly. Annual planning enables public and private sectors to reassess priorities and realign resources to meet changing needs.

Document Organization

The organization of the IT SSP represents a consensus outline based on IT SCC and IT GCC input. The following provides a mapping between the consensus outline and the SSP outline provided in the 2006 CI/KR Protection SSP Guidance to facilitate review by readers familiar with that format.

- **Section 1: Sector Profile and Goals.** Maps to SSP Guidance, Chapter 1: Sector Profile and Goals.
- **Section 2: Risk Management.** Maps to SSP Guidance, Chapter 2: Identify Assets, Systems, Networks, and Functions; Chapter 3: Assess Risk; and Chapter 4: Prioritize Infrastructure.
- **Section 3: Develop and Implement Protective Programs.** Maps to SSP Guidance, Chapter 5: Develop and Implement Protective Programs
- **Section 4: Information Sharing.** Maps to SSP Guidance, Chapter 8, Section 8.4, Information Sharing and Protection.
- **Section 5: CI/KR Protection Research and Development.** Maps to SSP Guidance, Chapter 7: CI/KR Protection Research and Development.
- **Section 6: Managing and Coordinating Sector Responsibilities.** Maps to SSP Guidance, Chapter 8: Managing and Coordinating SSA Responsibilities.
- **Section 7: Implementing the SSP and Tracking Progress.** Maps to SSP Guidance, Chapter 8: Measure Progress.

Each SSP section also includes two consistent elements—a callout box discussing the value proposition for public and private sector security partners and near- and long-term actions. Near-term (~1 year) and long-term (1-3 years) actions often have component subactions and may be tracked at that level through implementation. Appendix 5 summarizes the IT SSP actions. Although each near-term action may not be completed within the next year, it is expected that progress toward completing the action will occur within the next year (i.e., 2007-2008).

1. Sector Profile and Goals

This section describes the IT Sector, identifies the IT SSP's focus, establishes the sector's goals, and describes IT Sector security partners' roles and responsibilities.

1.1 Definition

Critical IT Sector functions support the Sector's ability to produce and provide high assurance IT products and services for a variety of sectors. Through the IT SSP development process, the Sector identified six critical functions:

- provide IT products and services;
- provide incident management capabilities;
- provide domain name resolution services;
- provide identity management and associated trust support services;
- provide Internet-based content, information, and communications services; and
- provide Internet routing, access and connection services.

These functions are distributed across a broad network of infrastructure, managed on a proactive basis and therefore able to withstand and rapidly recover from most threats.⁸

These critical IT Sector functions are provided by a combination of entities—often owners and operators and their respective associations—who provide hardware, software, IT systems, and services. IT services include development, integration, operations, communications, and security. IT Sector entities include the following:⁹

- Domain Name System (DNS) root and Generic Top-Level Domain (GTLD) operators;
- Internet service providers (ISPs);
- Internet backbone providers;
- Internet portal and e-mail providers;

The Internet encompasses the global infrastructure of packet-based networks and databases that use a common set of protocols to communicate. The networks are connected by various transports. The availability of the network and its services is the collective responsibility of the IT and Communications sectors.

⁸ Threat is defined as the intention and capability of natural or manmade (intentional or unintentional) events that would be detrimental to the IT Sector. This definition was developed by the IT Sector based on the terms and definitions in the NIPP.

⁹ Operating Charter of the Information Technology Sector Coordinating Council, January 24, 2006 <https://www.it-isac.org/documents/itscc/index.php>

- Networking hardware companies (e.g., fiber-optics makers and line acceleration hardware manufacturers) and other hardware manufacturers (e.g., personal computer (PC) and server manufacturers and information storage);
- Software companies;
- Security services vendors;
- Communications companies that characterize themselves as having an IT role;
- Edge and core service providers;
- IT system integrators; and
- IT security associations.

In addition, Federal, State, and local governments are a component of the IT Sector as providers of government IT services that are designed to meet the needs of citizens, businesses, and employees. The IT Sector includes public and private sector entities.

1.2 Scope

The IT SSP provides a framework for identifying and managing risk during steady-state (i.e., routine day-to-day) business operations to prevent, protect against, mitigate, and prepare for nationally significant events; technological emergencies; or presidentially declared disasters that threaten, disrupt, or cripple IT Sector infrastructure. Specifically, the IT SSP is concerned with all hazard events with cyber or physical consequences that:

- Cause, or are likely to cause, harm to mission-critical functions across the public and private sectors by impairing the confidentiality, integrity, or availability of electronic information, information systems, services, or networks; and/or
- Threaten public health or safety, undermine public confidence, have a negative effect on the national economy, or diminish the security posture of the Nation.

Such nationally significant events likely would affect communications and/or IT services in at least one region and possibly several regions of the country, including at least one major metropolitan area. Events would involve multiple communications service providers and/or IT products and services, resulting in a significant degradation of other essential infrastructures. Such an event would have an impact on the availability and integrity of communications and IT services for at least a significant portion of a business day or longer.¹⁰

Roles and Responsibilities

Private Sector:

- Own, operate, and provide IT Sector critical functions;
- Monitor IT Sector critical functions for abnormal events;
- Alert United States Computer Emergency Readiness Team (US-CERT) and others to any events that potentially threaten, disrupt, or cripple IT Sector infrastructure; and
- Work with the National Cyber Response Coordination Group (NCRCG) as appropriate to consider the implications of the event.

Government:

- Own, operate, and provide IT Sector critical functions (as applicable);
- Monitor government networks and systems for abnormal events;
- Alert US-CERT to any events that potentially threaten, disrupt, or cripple IT Sector infrastructure;
- Provide information to the NCRCG for its consideration; and
- Make a recommendation regarding whether an event involving cyber is nationally significant.

¹⁰ The discussion of the type of events that the IT SSP is concerned with is consistent with the NCRCG's Working Definition of a Cyber Incident of National Significance, December 2006. The NCRCG, a forum of 13 government agencies, coordinates intragovernmental and public-private preparedness and operations to respond to and recover from cyber incidents of national significance. The NCRCG is a key cyber incident management body that provides strategic assessments and ensures that appropriate Federal resources and capabilities are deployed to ensure an adequate response.

Identification of the scope of events that are of concern to the IT Sector is an important element of government and private sector efforts to identify, prioritize, and protect critical IT Sector functions. It provides a foundation for addressing overall preparedness, including prevention and protection under the IT SSP and understanding when to transition to Federally-coordinated response¹¹ and recovery under the NIMS and NRP.

1.3 Sector Security Goals and Objectives

Vision Statement for the Information Technology Sector

Public and private IT Sector security partners will continue building infrastructure resilience to support:

- *The Federal Government's performance of essential national security missions and preservation of general public health and safety;*
- *State and local governments' abilities to maintain order and to deliver minimum essential public services; and*
- *The orderly functioning of the economy.*

The IT Sector will continue to coordinate with other CI/KR sectors and work to ensure that any disruptions or manipulations of critical IT Sector functions are brief, infrequent, manageable, geographically isolated, and minimally detrimental to the welfare of the United States.

Public and private sector security partners collaborated to identify overarching Sector goals that support efforts to prevent, prepare for, protect against, mitigate, respond to, and recover from nationally significant events. These goals create a mutually beneficial framework to develop risk management and protective strategies that will enhance sector security. Pursuit of these goals requires action by a wide array of public and private security partners, including the commitment of expertise and the identification and prioritization of resources. IT Sector security partners will review these goals and progress toward implementing them annually. The goals and their associated objectives are described below in no particular order.

Goal 1: Prevention and Protection Through Risk Management. Identify, assess, and manage risks to the IT Sector's infrastructure and its international dependencies.

- **Objective 1.1:** Identify and annually review¹² critical IT Sector functions that support the Nation's security, economy, public health, and safety.
- **Objective 1.2:** Assess and prioritize risks to critical IT Sector functions, including evaluating emerging threats, vulnerabilities, and technology, and mapping them against the infrastructure to prioritize protective efforts.
- **Objective 1.3:** Tailor protective measures, which mitigate associated consequences, vulnerabilities, and threats, to accommodate the diversity of the IT Sector and develop and share IT security best practices and protective measures with security partners.
- **Objective 1.4:** Encourage IT Sector entities to exchange information about risk management strategies and foster a better understanding of how they improve the overall posture of the sector.

¹¹ For the purposes of the IT SSP, response refers to individual public and private sector entity and joint public and private sector activities to position the Sector to ensure that any disruptions or manipulations of the IT infrastructure are brief, infrequent, manageable, geographically isolated, and minimally detrimental to the welfare of the United States. Federally coordinated response will be specifically referenced as such.

¹² Critical IT Sector functions will be reviewed annually to determine if technological and environmental changes have occurred that alter the set of functions or their descriptions.

Goal 2: Situational Awareness. Improve situational awareness during normal operations, potential or realized threats and disruptions, intentional or unintentional incidents, crippling attacks (cyber or physical) against IT Sector infrastructure, technological emergencies and/or failures, or presidentially declared disasters.

- **Objective 2.1:** Collaborate, develop, and share appropriate threat and vulnerability information among public and private sector security partners, including development of indications and warnings.
- **Objective 2.2:** Expand strategic analytical capabilities that facilitate public and private sector security partner collaboration to identify potential incidents.

Goal 3: Response, Recovery, and Reconstitution. Enhance the capabilities of public and private sector security partners to respond to and recover from realized threats and disruptions, intentional or unintentional incidents, crippling attacks (cyber or physical) against IT Sector infrastructure, technological emergencies and/or failures, or presidentially declared disasters, and develop mechanisms for reconstitution.

- **Objective 3.1:** Develop and maintain communications, including establishing mechanisms and processes for communicating with other sectors during contingencies, and conduct annual tests of the resulting communication plans and programs.
- **Objective 3.2:** Develop and maintain incident response and coordination plans and procedures, and exercise them annually to ensure readiness and resilience.
- **Objective 3.3:** Develop plans, protocols, and procedures to ensure that critical IT Sector functions can be reconstituted rapidly after an incident.
- **Objective 3.4:** Collaborate with law enforcement to identify and mitigate criminal activities that have the potential to harm the sector’s infrastructure.

1.4 Partnering for Security

As set forth in the NIPP, the sector partnership model¹³ encourages the public and private sectors to collaborate on their respective CI/KR protection activities. This collaboration is accomplished through SCCs and GCCs, which form a national framework for coordinating CI/KR protection within and across sectors.

IT GCC Membership (as of December 2006)	
Department of Commerce • National Institute of Standards and Technology (NIST) • National Technology and Information Administration Department of Defense/Office of the Assistant Secretary of Defense for Networks and Information IntegrationDepartment of Homeland Security • Preparedness Directorate/NCSD (IT GCC Chair) • Preparedness Directorate/Office of Infrastructure Protection • Preparedness Directorate/(National Communications System (NCS) • Science and Technology Directorate	Department of JusticeDepartment of StateDepartment of the TreasuryOffice of the Director of National IntelligenceOffice of Management and Budget (OMB)Metropolitan Information ExchangeNational Association of State Chief Information Officers

¹³ For additional information on the Sector Partnership Model, see section 4 of the NIPP.

IT SCC Membership (as of December 2006)

BearingPoint	EWA Information and Infrastructure Technologies, Inc.	KPMG LLP
Bell Security Solutions, Inc.	IBM Corporation	Lockheed Martin
BellSouth Corporation	Information Systems Security Association	McAfee, Inc.
Center for Internet Security	Information Technology Association of America	Microsoft Corporation
Cisco Systems, Inc.	Information Technology Information Sharing and Analysis Center	NTT America
CA International, Inc.	Intel Corporation	R&H Security Consulting, LLC
Computer and Communications Industry Association	International Systems Security Engineering Association	Seagate Technology
Computer Sciences Corporation	Internet Security Alliance	Symantec Corporation
Computing Technology Industry Association	Internet Security Systems, Inc.	System 1, Inc.
Cyber Security Industry Alliance	Internet Security Trust and Privacy Alliance	TestPro
Electronic Industries Alliance	Juniper Networks, Inc.	Unisys Corporation
Entrust, Inc.		U.S. Internet Service Provider Association
		VeriSign
		Verizon

The IT SCC (composed of IT industry members) and the IT GCC (composed of government representatives) are the primary bodies for communicating their respective public and private perspectives and for developing collaborative policies, strategies, and security efforts to advance CI/KR protection. SCC and GCC representatives share experiences, ideas, best practices, and innovative approaches related to CI/KR protection and risk management for their respective sectors. In March 2006, the DHS established the Critical Infrastructure Partnership Advisory Council (CIPAC) to facilitate coordination and dialogue between the SCCs and GCCs. The various SCCs address cross-sector issues and interdependencies through their participation in the Partnership for Critical Infrastructure Security (PCIS). The IT SCC will coordinate with other sectors on cross-sector issues, such as cyber security, through forums such as the PCIS.

To achieve an integrated national plan, the DHS must coordinate with all security partners that have equities or interests in CI/KR protection. Public and private sector security partners are crucial not only to the implementation of this plan but also to the broader policy and operational relationships that enhance the IT Sector's overall security posture. Table 1-1 provides examples of IT security partners.

Table 1-1: Examples of IT Security Partners

Security Partner	Description
Office of Cyber Security and Communications	The office works to ensure the security, resilience, and reliability of the Nation's cyber and communications infrastructure in collaboration with the public and private sectors. The office is composed of the NCSD and the NCS. The DHS is designated as the SSA for the IT Sector. That responsibility is delegated to NCSD, which is responsible for coordinating with other government departments and agencies (through the IT GCC) and the private sector (through the IT SCC) to develop and implement the IT SSP. ¹⁴ The DHS also is designated as the SSA for the Communications Sector, with that responsibility delegated to NCS.
IT Government Coordinating Council	Chaired by NCSD and established in April 2005, the IT GCC collaborates with the IT SCC to plan, implement, and execute sector-wide security programs for the Nation's IT critical infrastructure.
Other Federal Departments and Agencies	The responsibilities of other Federal departments and agencies are distinct from the SSA's responsibilities. For example, under the Federal Information Security Management Act, the OMB and the NIST have responsibility for overseeing the security of, and providing guidance for, the Federal Government's IT assets, systems, networks, and functions. Federal law enforcement agencies, such as the Federal Bureau of Investigation (FBI), play a critical role in investigating threats and prosecuting the perpetrators of cyber and physical crimes. The intelligence community (IC) uses national-level intelligence capabilities and resources to identify and counter threats. Law enforcement and the IC provide early warning or potential target information that can help the IT Sector and homeland security community implement preventive and protective measures.
State and Local Governments	State and local governments provide IT services that fulfill the needs of their citizens, businesses, and employees. The National Association of State Chief Information Officers (NASCIO), which represents the senior IT leaders for each State, is a key security partner of the IT Sector. State government participation in the IT SSP is achieved through the representation of NASCIO on the IT GCC. Local government participation in the IT SSP is achieved through the representation of the Metropolitan Information Exchange on the IT GCC.
IT Sector Coordinating Council	Established in January 2006, the IT SCC addresses policy and strategy issues and advises government counterparts on sector CI/KR protection issues. The IT SCC is self-organized, self-run, and self-governed. It enables owners and operators to coordinate on a wide range of sector-specific strategies, policies, activities and issues. ¹⁵
IT-ISAC	The IT Information Sharing and Analysis Center (IT-ISAC) offers its private sector members a current and coherent picture of the security posture of the IT infrastructure. ¹⁶ In addition to these policy coordination bodies, the IT Sector also relies on the IT-ISAC to provide operational and tactical capabilities for sharing information.
Private Sector Owners and Operators	Owners and operators of IT CI/KR implement infrastructure protection practices as part of their routine business risk management activities and play a crucial role in the security of the IT Sector.
Communications Sector	Recognizing the growing convergence of IT and communications and their significant interdependencies, the IT Sector coordinates closely with the Communications Sector. ¹⁷ Partnering with the Communications Sector is especially important for exchanging information about the Internet infrastructure, a responsibility shared by both sectors.
Other CI/KR	IT Sector security partners understand how consumers use their products and services and recognize the cyber security challenges that they face. Although the cyber security practices for specific CI/KR are best addressed within their respective sectors, IT Sector security partners coordinate and work with other sectors to articulate and address the interdependence among the infrastructures as part of managing IT Sector risks.

¹⁴ For additional information about the roles and responsibilities of the IT SSA, see section 6.

¹⁵ For additional information about the roles and responsibilities of the IT SCC, see section 6.

¹⁶ For additional information on the IT-ISAC, see section 4.

¹⁷ Commonalities across both sectors' membership facilitate the coordination.

Security Partner	Description
Other ISACs	ISACs provide a trusted mechanism for information sharing within and among CI/KR. The National Coordinating Center (NCC) for Telecommunications, as the ISAC for the Communications Sector, is a well-established information-sharing center with a 24 hours per day, 7 days per week (24/7) operations center for monitoring threats and exchanging information between Communications Sector members and other interdependent critical infrastructure sectors (e.g., IT Sector). The Multi-State ISAC (MS-ISAC) provides a mechanism for information sharing and outreach to State and local governments regarding cyber security issues. ¹⁸
Foreign Governments and International Organizations	Because the IT Sector is global in nature, interconnected, and interdependent, international partners play a key role in the prevention, protection, response, and recovery of critical IT Sector functions. Establishing and maintaining consistent and reliable relationships with international partners is vital to ensuring the security of the sector.

1.5 Authorities

Authorities addressing such issues as homeland security, national security, privacy, and IT audits affect or influence the IT Sector and provide direction to public and private sector security partners. Because of the interconnectedness of the IT and Communications Sectors, many authorities applicable to telecommunications are relevant to IT as well. Key authorities address the availability, resilience, and security of the infrastructure.

Appendix 2 presents an overview of key authorities that provide the foundation for IT Sector policies and regulations in the United States and guidance on sector coordination. These authorities—some of which apply to the Federal Government and others to the private sector—govern the collection, sharing, and protection of information, conduct of vulnerability and risk assessments, and the identification, development, and implementation of protective strategies and programs.

1.6 Actions

The following bulleted list includes near term and long term actions to be completed to implement this section of the SSP.

1.6.1 Near Term (~1 year)

- Facilitate the development of and articulate for IT Sector members the national security and business value for participation in SSP implementation activities. (NCSD, SCC, and GCC)
- Develop criteria that may be used for determining nationally significant events. (NCSD, SCC, GCC, and NCRCG) (Underway)
- Provide input into national-level efforts to clarify the roles and responsibilities of public and private sectors in Federally coordinated response, recovery, and reconstitution efforts involving nationally significant events. (NCSD, SCC, GCC, and NCRCG)
- Provide public and private sector perspectives and input to assist in planning for Federally coordinated response and recovery efforts involving nationally significant events. (NCSD, SCC, GCC, and NCRCG input)

¹⁸ See section 4 for additional information about the MS-ISAC and its relationship to the IT Sector.

1.6.2 Long Term (1-3 years)

- Conduct exercises that test the implications of a nationally significant event and the resulting public and private sector roles, responsibilities, and capabilities. (NCSD, SCC, GCC, and NCRCG)
- Annually review and revise IT SSP goals, objectives, and authorities. (GCC and SCC)
- Hold joint IT and Communications sectors meeting biannually to address issues of interest to both sectors, and discuss potential areas for collaboration. (NCSD, NCS, SCC, GCC, Communications SCC, and Communications GCC)
- Work in partnership through the PCIS with the Communications Sector to help other CI/KR understand their dependence on the IT and Communications Sectors. (NCSD, NCS, SCC, GCC, Communications SCC, and Communications GCC)

2. Risk Management

Individual IT Sector entities routinely manage a wide range of risks to ensure the delivery of products and services to support their customers. Despite these individual entities' efforts, there is not yet a national-level understanding of risk faced by the IT Sector. Public and private sectors are collaborating to address these broader risks that could affect the ability of the sector's critical functions to support the economy and national security. The sector-wide risk approach describes how risk will be evaluated across the IT Sector focusing on critical IT Sector functions; it is not guidance for individual entities' risk management activities. A sector-wide risk assessment will help determine the all-hazards risk profile for the IT Sector, focus resource allocation for protection for the IT Sector to manage its inherent risks, and increase awareness of risks across public and private sectors.

Because this is the first effort to assess sector-wide risks, the approach outlined in this section is high level and will evolve and mature through implementation. Future iterations of the IT SSP should reflect a more detailed approach that expands on the concepts in this version.

The IT SCC and IT GCC convened a working group to address the challenge of developing an approach to assess and manage IT Sector risks. The effort considered leading risk management approaches, methodologies, and tools currently employed by sector entities. Given the IT Sector's complexity, global nature, and unique character, the most viable way to proceed is with a qualitative, top-down approach that considers sector security goals and objectives, and then identifies critical IT Sector functions. The resulting sector-wide risk approach focuses on those IT functions with national consequence and is intended to meet and fulfill Sector Goal 1, Prevention and Protection Through Risk Management.

The IT Sector's risk approach fulfills the intent of the NIPP risk management framework by adapting and modifying its activities and concepts to address the unique IT Sector risk environment. The risk assessment approach leverages the baseline criteria outlined in the NIPP, which specify that risk assessment methodologies include an analysis of the human, cyber, and physical elements¹⁹ of infrastructure. In all cases, the human, cyber, and physical elements are assessed in the context of their criticality

Value Proposition

Coordination of risk management activities by public and private IT Sector security partners should leverage their respective knowledge and expertise while helping focus efforts and resources on ensuring the continued availability of critical IT Sector functions. This process combines individual organizational risk management goals and activities with a perspective and collaborative approach that is nationally significant. Acknowledging and addressing differences between individual and organizational objectives and those of the sector-wide approach offers value by providing individual owners, operators, and security partners with an understanding of the sector perspective and a means to manage IT Sector risk effectively and consistent with national priorities.

¹⁹ Physical elements of infrastructure include tangible property; cyber elements include electronic information and communication systems, and the information contained therein; human elements include critical knowledge of functions, people uniquely susceptible to attack, or the social aspects of infrastructure protection.

to the sector as a whole and the potential for their disruption, damage, or loss to affect the sector. Throughout this section, a common set of terms will be used to describe the IT Sector's risk assessment approach (see text box).²⁰

2.1 Background of the IT Sector's Risk Environment

The IT Sector's risk environment is inherently complex and dynamic. A few primary characteristics shape the evolving risk environment: interdependencies between the IT Sector and other critical infrastructure sectors; the highly diverse, virtual, interconnected, and international nature of the IT infrastructure; and the constantly changing threat landscape. The sector has global operations that are interdependent and interconnected with other infrastructures. These operations enhance efficiency and effectiveness and increase the resilience of the sector; however, they daily face numerous multifaceted global threats from natural and manmade events. Many of these threats occur frequently but do not have significant consequences because of individual entities' existing security and response capabilities. However, some of these threats are strategic and could affect critical IT Sector functions. The high degree of interdependency of the IT Sector, its interconnectedness, and non-traceable and unidentifiable actors makes identifying threats, assessing vulnerabilities, and estimating consequences difficult and must be dealt with in a collaborative and creative manner.

2.1.1 Various Entities' Risk Management Approaches

Risk management approaches used throughout the IT Sector are based on various philosophies, methodologies, and tools. Private sector entities typically base their approaches on business objectives, such as shareholder value, efficacy, and customer service. Regulatory compliance requirements associated with financial reporting integrity and privacy initiatives are increasing awareness across entities within the sector of risk management strategies.

As part of their individual risk management approaches, many IT Sector entities have designated focal points for risk management and/or security. Some have chosen to centralize this function within their organizations while others have chosen to have it distributed across their operations. In addition, IT Sector entities assess various types of risk (e.g., financial, human, supply chain, legal, and compliance) through multiple approaches (e.g., quantitative, qualitative, and modeling and simulation) leveraging both commercial and government off-the-shelf products and customized tools. These entities use a variety of common risk management frameworks to proactively manage steady-state risk (see text box). The list is not all inclusive and not intended to endorse any approach; rather, it is provided as a resource to increase awareness of various methods in use by some sector entities. Appendix 2 provides additional detail on these frameworks.

Terms

- **Risk:** The expected magnitude of loss resulting from an incident (e.g., terrorist attack, natural disaster) and with the likelihood of such an event occurring and causing that loss.
- **Risk Management:** A planning methodology that outlines the process for setting security goals; identifying assets, systems, networks, and functions; assessing risks; prioritizing and implementing protective programs; measuring performance; and taking corrective action.
- **Threat:** The intention and capability of natural or man-made (intentional or unintentional) events that would be detrimental to the IT Sector.
- **Vulnerability:** A property or characteristic of a function, process, or supporting asset, system, or network that can be exploited for unintended use or can be disrupted by a natural hazard or technological failure.
- **Consequence:** The level, duration, and nature of the loss resulting from the incident.
- **Assurance:** Measure of confidence that the security features, practices, procedures, and architecture of IT Sector products and services accurately mediates and enforces the security policy.

²⁰ Although numerous definitions of the terms exist (e.g., from NIST and the International Organization for Standardization (ISO)), the IT SSP bases the terms and definitions on those in the NIPP because the SSP is an annex of that document. The assurance definition is taken from the National Information Assurance Group. Occasionally, the definitions are modified to represent the unique considerations of the sector.

Although outside the scope of this chapter, these individual risk management efforts are designed to support organizational business objectives and, in aggregate, they enhance the security and resilience of the Sector as a whole. A more holistic approach; however, is needed that considers the IT Sector’s ability to support the economy and national security.

2.2 Developing an IT Sector Risk Profile

To develop the overall IT Sector risk profile, designated public and private sector security partners will identify critical sector functions collaboratively, analyze threats to those functions, assess vulnerabilities, evaluate consequences, and identify mitigations. A top-down approach will be taken that considers sector goals and objectives to assess whether the current level of risk is acceptable or whether further mitigation is needed in the form of protective programs or other mechanisms designed to reduce risk to an acceptable level. This top-down approach, which focuses on understanding the functions of the infrastructure rather than cataloging physical fixed assets, was determined to be more effective for the highly distributed IT infrastructure. The result is a qualitative assessment of sector-wide risks that public and private IT Sector security partners can use to prioritize additional mitigations and protective measures. Coordination of risk management activities by IT Sector security partners should help focus efforts and resources on ensuring the continued availability of critical IT Sector functions, products, and services and improved resilience of the nationally critical IT infrastructure. This dynamic relationship will be assessed through iterative analysis and is demonstrated in figure 2-1.

Common Risk Management Frameworks

- Control Objectives for Information and Related Technology (COBIT) 3.0/4.0
- Disaster Recovery Institute International (DRII)
- International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27000 Series, Information technology—Security techniques—Information security management systems
- ISO/IEC 13335, Information technology—Security techniques—Management of information and communications technology security—Part 1: Concepts and models for information and communications technology security management
- ISO/IEC 17799, 2005 Information technology—Security techniques—Code of practice for information security management
- ISO/IEC 21827, Systems Security Engineering—Capability Maturity Model (SSE-CMM®)
- Information Technology Infrastructure Library (ITIL) Security Management
- NIST Special Publication 800-12, An Introduction to Computer Security: The NIST Handbook
- NIST Special Publication 800-30, Risk Management Guide for Information Technology Systems
- NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems
- Operationally Critical Threat, Asset, and Vulnerability EvaluationSM (OCTAVESM)

Figure 2-1: Developing the IT Sector Risk Profile



The sector-wide approach is not designed for use by individual entities and will not arrive at the level of detail of the entities' risk efforts discussed in section 2.1.1. Rather, the approach in the IT SSP examines entities' functions in the context of understanding the risk that could potentially translate to the broader IT infrastructure. To the extent possible, the approach will leverage the entities' existing efforts and best practices across the sector and adapt them to address the IT infrastructure as a whole. This approach will enable individual entities to better understand the impact of their respective risk management strategies on the sector's security posture. By combining individual organizational risk management goals and activities with a perspective and collaborative approach that is nationally significant, the overall security and resilience of the IT Sector is further enhanced.

2.2.1 National IT Sector Risk Management Approach

Successful implementation of the top-down qualitative approach to assessing IT Sector risk depends on collaboration between public and private sector security partners. The risk management approach includes the following steps:

1. Identifying critical functions;
2. Assessing threats, vulnerabilities, consequences, and mitigations:
 - a. Analyzing threats;
 - b. Assessing vulnerabilities;
 - c. Evaluating consequences; and
 - d. Identifying mitigations; and
3. Prioritizing risks for the overall sector profile.

Sections 2.3 through 2.5 describe the steps listed above in detail.

2.3 Identifying Critical Functions

The IT infrastructure is an aggregate of primarily virtual and distributed functions supported by various assets, systems, and networks. The distributed nature of the infrastructure inherently provides physical and virtual resilience; however, some functions may have limited supporting cyber, physical, and human elements of the infrastructure that could present risk and potentially increase their vulnerability. Where risk is identified, the Sector will use the assessment process to raise awareness among the entities that rely on the critical functions and propose specific protective capabilities to mitigate risk, where appropriate.

Functions are sets of processes that produce, provide, and maintain products and services. IT Sector functions encompass the full set of processes (e.g., research and development, manufacturing, distribution, upgrades, and maintenance) involved in transforming supply inputs into IT products and services. These functions support the Sector's ability to produce and provide high-assurance products, services, and practices that are resilient to threats and can be rapidly recovered. Assurance is essential to achieving the Sector's vision and is therefore a fundamental aspect of all critical functions. The sub-functions of the critical functions each directly address this aspect and also work in concert to consistently create high-assurance products and services. The IT Sector's functions are not limited by geographic or political boundaries, increasing the need for international collaboration and coordination for not only risk assessment activities but also best practices and protective program design and implementation.

2.3.1 Screening and Assessing Consequences

A top-down approach to assessing functions results in identifying only those functions that meet a minimum consequence threshold. Resources then can be devoted to analyzing nationally consequential functions and their supporting infrastructure.

Criticality of IT Sector functions is assessed based on their potential impact on government or sector missions independent of any specific defined threat scenario (addressed in section 2.4.1). The criticality of a function depends on many factors, such as tolerable magnitude and duration of loss or degradation of that function. The resilience of functions to disruption or degradation increases with the availability of substitutes for the products and services resulting from a given critical function, with the degree of diversity that exists within the functions' processes and with diversity of providers. A disruption or degradation of a function can have a cascading effect if other functions are highly dependent on its outputs. Functions with high dependence and interdependence are of particular concern in this assessment.

IT Sector functions will be screened and prioritized based on HSPD-7 consequence categories and criteria for evaluating nationally significant events. These criteria include the following:

- **Governance Impact:** Effects on Federal, State, and local governments;
- **Economic Security Impact:** Effects on users and the greater economy;
- **Public Health and Safety Impact:** Effects on human health from injuries and loss of life; and
- **Public Confidence Impact:** Effects on the public's morale, caused by the visibility of the impact, number of people affected, and length of time needed to switch to alternative sources.

Table 2-1 identifies critical IT Sector functions²¹ and their descriptions based on the consequence criteria described above. These functions are required to maintain or reconstitute the network (e.g., the Internet, local networks, and wide area networks) and its associated services. The list represents IT SCC and IT GCC consensus on critical IT Sector functions that are vital to national and economic security and public health, safety, and confidence.

Table 2-1: Critical IT Sector Functions and Descriptions

IT Sector Function	Description
Provide IT Products and Services	The IT Sector conducts operations and services that provide for the design, development, distribution, and support of IT products (hardware and software) and operational support services that are essential or critical to the assurance of national and economic security and public health, safety, and confidence. These hardware and software products and services are limited to those necessary to maintain or reconstitute the network and its associated services.
Provide Incident Management Capabilities	The IT Sector develops, provides, and operates incident management capabilities for itself and other sectors that are essential or critical to the assurance of national and economic security and public health, safety, and confidence.
Provide Domain Name Resolution Services	The IT Sector provides and operates domain registration services, top-level domain (TLD)/root infrastructures, and resolution services that are essential or critical to the assurance of national and economic security and public health, safety, and confidence.
Provide Identity Management and Associated Trust Support Services	The IT Sector produces and provides technologies, services, and infrastructure to ensure the identity of, authenticate, and authorize entities and ensure confidentiality, integrity, and availability of devices, services, data, and transactions that are essential or critical to the assurance of national and economic security and public health, safety, and confidence.

²¹ These are public and private sector consensus critical IT Sector functions for government fiscal year 2007. Annual planning enables the review and update of these functions to reflect changes in the IT Sector environment.

IT Sector Function	Description
Provide Internet-based Content, Information, and Communications Services	The IT Sector produces and provides technologies, services, and infrastructure that deliver key content, information, and communications capabilities that are essential or critical to the assurance of national and economic security and public health, safety, and confidence.
Provide Internet Routing, Access, and Connection Services	The IT Sector (in close collaboration with the Communications Sector) provides and supports Internet backbone infrastructures, points of presence, peering points, local access services, and capabilities that are essential or critical to the assurance of national and economic security and public health, safety and confidence.

2.3.2 Decomposing Critical IT Sector Functions

The IT Sector's approach will decompose the critical IT Sector functions to identify the processes or operations necessary to produce or provide that function. This technique breaks down the functions to a more practical level for analysis, focuses risk assessment efforts on only those processes essential for those functions, and facilitates the understanding of dependencies between processes and their supporting assets, systems, and networks. The IT Sector's approach will decompose its functions by describing the high-level processes generally required to transform inputs into outputs with public and private sector security partners involved in producing or providing the functions.

2.4 Assessing Threats, Vulnerabilities, Consequences, and Mitigations

The IT Sector's approach will evaluate threats to the critical functions, identify associated vulnerabilities, assess consequences, assess the effectiveness of mitigations that are already in place, and identify new or enhanced capabilities needed to manage sector risk effectively. To provide comparable risk assessment results from a sector perspective, consistent measurements will be used for evaluating threats, vulnerabilities, consequences, and mitigations.

2.4.1 Analyzing Threats

IT infrastructure is confronted by various threats; therefore, the threat analysis approach will consider the following spectrum of intentional and unintentional manmade and natural threats:

- Natural threats (e.g., hurricane, fire, floods);
- Cyber threats (e.g., bot networks, data corruption);
- Workforce threats (e.g., pandemic flu, insider threat, industrial espionage, human error);
- Terrorist threats (e.g., chemical and biological attacks); and
- Supply chain threats (e.g., manufacturing plant destruction).

Threats that affect critical IT Sector functions will be assessed for the high-level critical functions themselves and for functions' critical processes. The assessment also will consider policy and operational aspects of each threat and the criteria to determine when a threat is of national concern for IT Sector security partners.

Traditional threat analysis generally identifies an actor and the actor's intentions, motives, and capabilities to compromise a given target. Such approaches typically rely on historical data associated with a particular actor to predict threats. When analyzing threats to the IT Sector, this traditional approach to threat assessment alone is not sufficient in the sector's risk environment because actors are not easily identifiable or traceable, and attacks can go from conception to exploitation within hours. The IT

Sector's approach will complement the traditional threat assessment approach with additional factors based on capabilities and intent independent of known actors to consider emerging nontraditional threats.

The IT Sector's approach will analyze threats that have national significance based on capabilities. The sector defines threat capability as the availability of and/or the ease of use of tools or methods that potentially could be used to damage, disrupt, or destroy critical IT Sector functions. With respect to natural threat, capability is inherent; therefore, natural threats that could have a nationally significant impact will be considered. A capabilities-based approach is applied differently for intentional man-made threats. For intentional manmade threats, the IT Sector is particularly concerned about widely available tools or methods that can be configured easily to exploit critical IT Sector functions. The sector also is vulnerable to unintentional manmade threats because of its high reliance on human interaction and skill sets. The IT Sector's threat approach will include trend analysis of historical data and assessment of capabilities that could destroy, incapacitate, or exploit critical IT Sector functions.

Working together, public and private IT Sector security partners will create strategic and operational threat scenarios based on capability and intent and assess them against critical IT Sector functions. The IT Sector is subject to various threats; consequently, various scenarios will be included in the assessment.

An accurate threat assessment requires collaboration among IT Sector security partners, such as the private sector, the DHS, and other IC partners. Accurately analyzing threats depends on public and private sector security partners generating requirements for collection of threat data and sharing relevant threat information. For example, the DHS through the Homeland Infrastructure Threat and Risk Analysis Center (HITRAC)²² and working in partnership with other IC partners, intends to provide specialized classified and unclassified analytical threat products in the form of threat warnings, incident reports, strategic planning information, target selection matrices, attack-specific threat scenarios, and overall sector-specific threat assessments. Public and private sector security partners are discussing how HITRAC can support the IT Sector threat assessment through future collaboration and requirements development to demonstrate value for customers. Private sector security partners provide a comprehensive understanding of the evolving technological capabilities for emerging threats, their associated consequences, and potential targets. Annually, IT Sector public and private sector security partners will analyze potential threats and determine those of national significance for IT Sector risk assessment.

2.4.2 Assessing Vulnerabilities

To assess vulnerability of the critical functions, the IT Sector's approach will examine associated processes for characteristics that may be exploited by the threat scenarios resulting from the previous step of the risk assessment. Vulnerabilities that, if exploited, could have national consequences are identified and paired with their respective function processes.

Each threat scenario is applied to critical functions' processes and assessed against a set of vulnerability categories (e.g., people, process, and technology). Although these vulnerability categories may intersect or overlap in some cases, the following descriptions will help guide the identification of vulnerabilities:

- **People:** Vulnerabilities associated with critical knowledge of functions, workforce resources susceptible to intentional threats, and the social aspects of infrastructure protection. This category considers factors affecting the workforce such as human resource practices (e.g., personnel security), demographics (e.g., citizenship, qualifications), training and education (e.g., quality and quantity of institutions that teach and train the workforce), and market environment(s) (e.g., compensation and benefits).
- **Processes:** Vulnerabilities associated with the sequence and management of operations or activities. This category includes factors such as manufacturing, logistics, and information flow (e.g., quantity and throughput of distribution channels), con-

²² HITRAC serves as a national fusion center, bringing together intelligence and infrastructure specialists to integrate, analyze, and share strategic and national-level information regarding the threat of terrorist attack against U.S. CI/KR, including IT and cyber infrastructures. HITRAC capabilities also are discussed in section 4 and appendix 3.

tingency planning and process flexibility (e.g., continuity of operations), and efficiency and effectiveness (e.g., information access globalization).

- **Technologies:** Vulnerabilities associated with integration of technologies within critical functions. This category includes factors such as reliance on hardware and software (e.g., availability, security), and system dependencies and interdependencies.

When identifying vulnerabilities, the sector's approach also will assess the likelihood that the threat scenario will successfully exploit a vulnerability. To ensure a valid assessment of likelihood, the effectiveness of existing mitigations also will be considered. This process will assist the sector in determining where vulnerabilities have been addressed already and where additional mitigations may be appropriate.

2.4.3 Evaluating Consequences

The potential consequences associated with nationally significant events represent the expected range of direct and indirect impacts that could occur should a threat exploit unmitigated vulnerabilities in critical IT Sector functions. The interdependency between the physical and cyber elements of the infrastructure is of particular concern for public and private IT Sector security partners. Conversely, disruption or degradation of cyber elements can have physical consequences as well (e.g., the failure of a control system managing a manufacturing process for IT products). In addition, dependencies and interdependencies between and among critical IT Sector functions will be evaluated and factored into sector risk assessment efforts.

Using HSPD-7 consequence categories and criteria for evaluating nationally significant events, the IT Sector's approach to consequence assessment identifies impacts on national and economic security and public health, safety, and confidence should a critical function be disrupted or degraded. The assessment may consider such questions as, If this function or process is disrupted or degraded:

- Is there a potential for loss of life, injuries, or adverse impact on public health and safety?
- How many users could be severely affected?
- What are the economic impacts, including asset replacement, business interruption, and remediation costs?
- Will Federal, State, and/or local governments be adversely affected? If yes, how much time might elapse before the impact is realized?
- What is the maximum amount of time that the function or process can be disrupted or degraded and still meet the minimal needed functionality in a timely manner?
- Is it possible to switch to alternate source(s)? If yes, how much time is required?

Private sector security partners will collaborate to identify the most appropriate methods for evaluating functions' consequences for their organizations and how best to share the relevant findings with the public sector security partners. Similarly, public sector security partners will collaborate to evaluate functions' consequences from a government perspective. The results of these evaluations then will be combined to understand the overall impacts to the infrastructure.

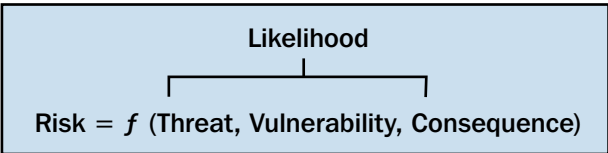
2.4.4 Identifying Mitigations

Private sector entities implement a vast array of mitigations primarily based on their organizational objectives, whereas public sector interests are focused on assuring the ability of critical IT Sector functions to support the economy and national security. Understanding how existing public and private sector risk mitigations work together to address risks collectively and identifying additional capabilities is an essential component of the IT SSP risk management approach. These capabilities will be considered as part of the process for identifying and implementing new protective programs described in section 3.

The risk assessment approach assesses existing mitigations that reduce threats, vulnerabilities, and consequences, and identifies opportunities for new and enhanced risk mitigation capabilities. These opportunities may exist because of differences between individual organizational objectives and those of the sector-wide approach. Acknowledging and addressing these differences provides value by enabling individual owners, operators, and security partners to understand the sector perspective and manage risk effectively across the sector. Sector-wide risk management activities focus on mitigating, transferring, or accepting risks. At this level, public policy also can be influenced and incentives can be developed for private sector entities to consider a national or sector-wide perspective in their risk management activities.

2.5 Prioritizing for the IT Sector Risk Profile

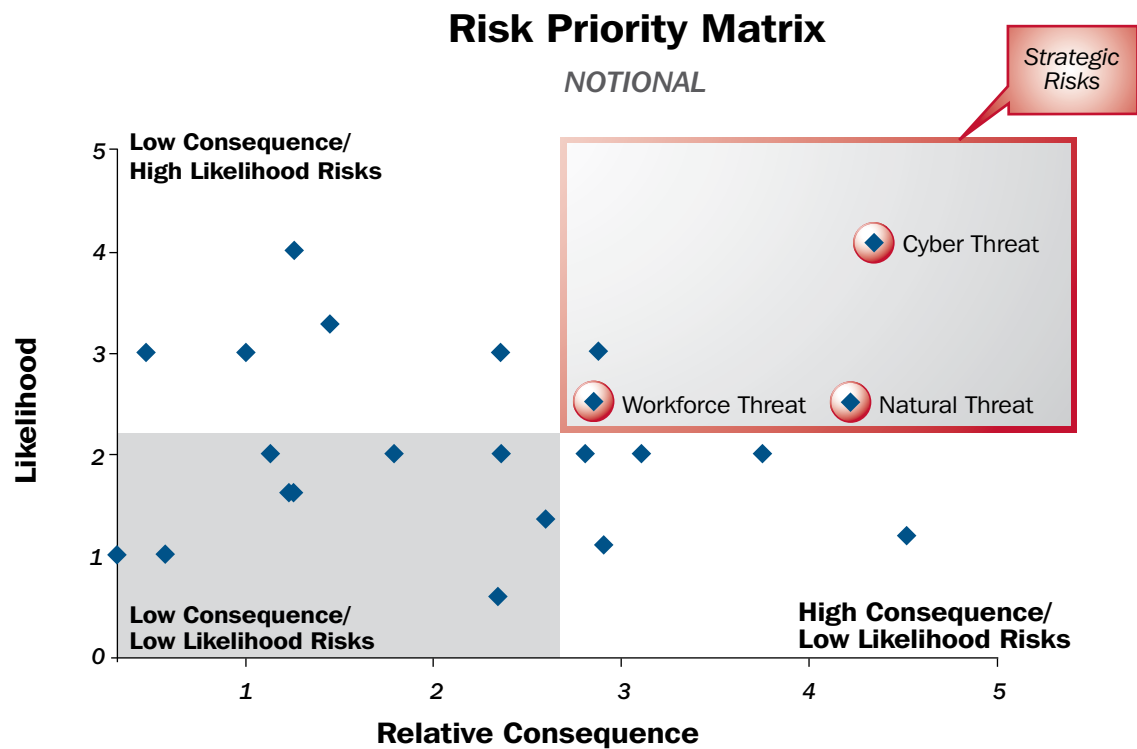
The basic qualitative formula for risk defines risk as a function of threat, vulnerability, and consequence. Threat and vulnerability combined represent the likelihood that a vulnerability could be exploited successfully by a threat.



Because limited resources exist to manage the wide range of IT Sector risks, it is important that public and private sector security partners agree on how to best prioritize risks and apply resources to ensure that critical IT Sector functions are protected.

To help determine how to allocate resources, risk priorities will be illustrated on a matrix using consequence and likelihood that a vulnerability will be successfully exploited by a threat. Figure 2-2 demonstrates how threat scenarios may be ranked in relation to one another based on their risk. The IT Sector’s approach will focus primarily on strategic risks in the upper right-hand quadrant—those with a high consequence/high likelihood rating.

Figure 2-2: Notional Risk Priority Matrix



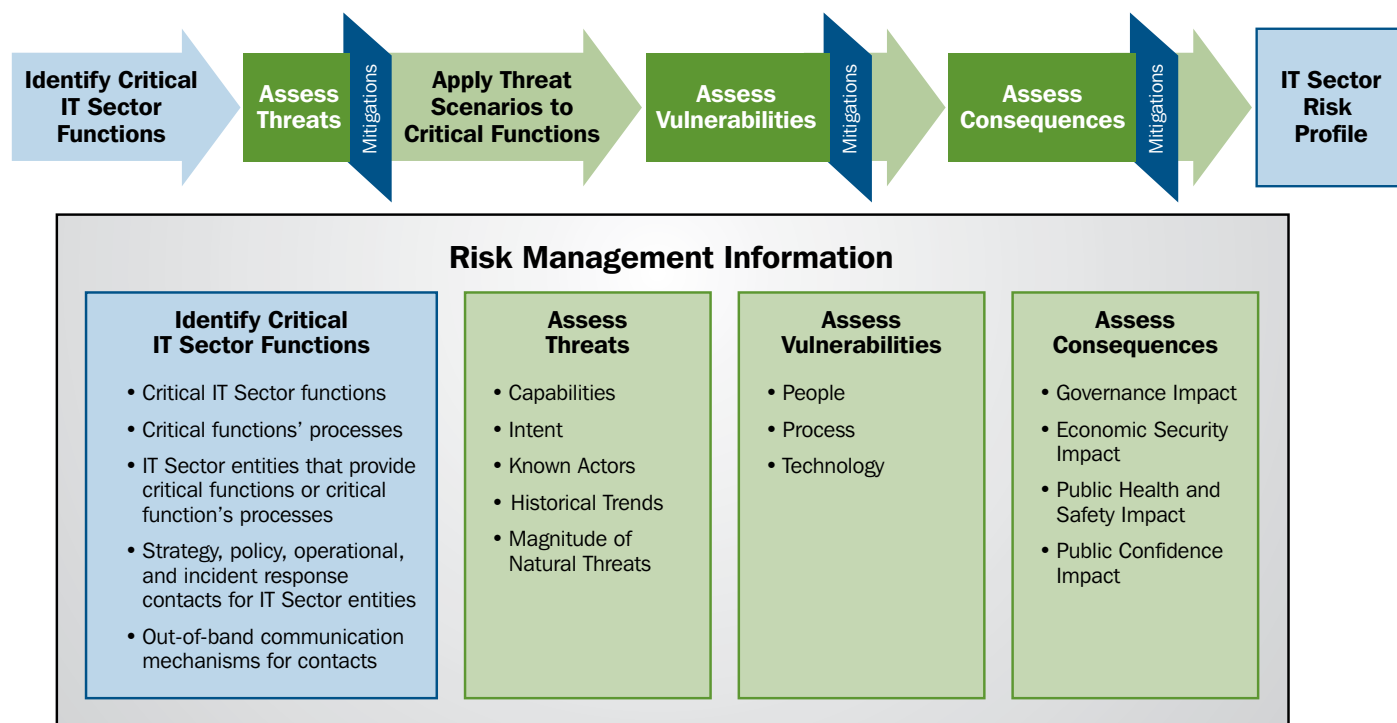
Prioritizing IT Sector risks depends on using consistent measurements for evaluating nationally significant events, comparing results from a sector-wide perspective, and using specific infrastructure information to validate the results. The IT Sector's approach to prioritization will become more defined after completion of actions associated with measurements and thresholds for threats, vulnerabilities, and consequences and described in section 2.7. As such, prioritization will be addressed in greater detail in future versions of the IT SSP.

2.6 Risk Management Information

The implementation of the IT Sector's risk management approach requires commitment from public and private sector security partners. Without active participation of both, the resulting IT Sector risk profile and risk management activities would be inaccurate and ineffective. A collaborative group of public and private sector security partners will implement the national IT Sector risk management approach. Because this group will consist of public and private sector members exchanging operational information, the CIPAC will be used to create a trusted environment for sharing and to afford the protections of the Federal Advisory Committee Act associated with CIPAC. In addition, the sector recommends that a secure Web-based tool be developed to facilitate the sector-wide collaboration necessary to implement the approach and to reach a broader audience of IT Sector entities essential to ensuring the availability and/or reconstitution of the critical functions.

The IT SCC and IT GCC acknowledge that sharing and updating information and assessments of threats, vulnerabilities, consequences, and mitigations are essential to developing a valid IT Sector risk profile. Information needs have been developed collaboratively to ensure that the analysis focuses only on critical IT Sector functions, the specific threats that are being assessed, vulnerabilities that could be exploited by those threats, and the consequences of such events. Figure 2-3 summarizes the composite information derived from a public and private sector partnership needed to support the development of the IT Sector risk profile.

Figure 2-3: Risk Management Information



IT Sector entities' assets supporting the critical functions will be neither requested nor collected as part of this process because the availability, security, and reconstitution of such assets are the responsibility of those entities. The virtual and distributed nature of critical IT Sector functions also makes cataloguing assets impractical and would not yield meaningful results. IT private sector security partners recognize the need to identify and manage information needed to develop the IT Sector risk profile and will accomplish that objective in an arrangement that considers their capabilities, resources, and concerns about the management and protection of such information. The IT SCC and IT GCC will determine the appropriate entity to manage and protect risk management infrastructure information. IT private sector security partners recommend considering use of the IT-ISAC²³ to manage and protect this information because of the proven and trusted relationship, reinforced by contractual obligations, that exists between the IT-ISAC and private sector entities. The actions described in section 2.7 provide additional detail about the roles of public and private sector security partners in identifying and providing this information.

2.7 Actions

The following bulleted list includes near term and long term actions to be completed to implement this section of the SSP.

2.7.1 Near Term (~1 year)

Actions to Develop the IT Sector Risk Profile

- Develop an implementation plan for the 2007 IT Sector Risk Profile. (NCSD with GCC and SCC input)
- Identify resources needed to implement the 2007 IT Sector Risk Profile. (NCSD with GCC and SCC input)
- Select the appropriate entity to manage and protect IT Sector risk management information. (SCC, IT-ISAC, and GCC)
- Decompose the sector's critical functions and/or sub-functions. (SCC, IT-ISAC, and GCC)
- Develop initial draft measurements and thresholds for evaluating consequences, vulnerabilities, and threats consistently to enable comparable risk assessment results. (SCC and IT-ISAC with GCC input)
- Initiate the identification of the sector's nationally consequential threats, and conduct analysis of them against the critical IT Sector functions. (GCC, IT-ISAC, HITRAC, and IC)
- Initiate the identification and assessment of vulnerabilities and consequences for critical IT Sector functions. (IT-ISAC with GCC input)
- Initiate the identification and assessment of mitigations that address threat, vulnerability, and/or consequences. (IT-ISAC and GCC)
- Collaborate with the Communications Sector regarding the identification and risk assessment of the Internet infrastructure, including specifically physical and cyber threat assessments for the Internet. (SCC, IT-ISAC, and GCC)

Other Actions:

- Continue to encourage participation in the IT SCC and IT GCC. (SCC, IT-ISAC, and GCC)
- Encourage IT Sector entities to consider adopting individual risk management approach(es) appropriate for their unique operating environments. (SCC and IT-ISAC)
- Collaborate and coordinate with the other CI/KR sectors to address threats outside the IT Sector's control. (SCC, IT-ISAC, and GCC)

²³ Section 4, Information Sharing, provides additional detail about the IT-ISAC.

2.7.2 Long Term (1-3 years)

- Review (annually) critical IT Sector functions to determine if technological and environmental changes have occurred that alter the set of functions or their descriptions. (SCC and GCC)
- Identify (annually) threats, vulnerabilities, consequences, and mitigations that are of national significance to the sector. (SCC, IT-ISAC, GCC, HITRAC, and IC)
- Define and refine the IT Sector risk profile over time as the approach described in this section is implemented and repeated. (GCC, SCC, HITRAC, and IC)
- Improve cross-sector coordination. (SCC, IT-ISAC, and GCC)

3. Develop and Implement Protective Programs

Protective programs include measures or activities that are undertaken by various security partners to prepare for, prevent, protect against, respond to, and recover from incidents that have the potential to affect critical IT Sector functions. Programs are sponsored and/or led by public or private sector security partners, or they represent a partnership between the public and private sectors. Protective programs facilitate progress toward achieving the sector's goals. Protective programs are characterized by actions to:

- Define needs and objectives to ensure efforts are comprehensive and sustainable;
- Respond to the needs of various security partners;
- Apply appropriate resources in a cost-effective and efficient manner (e.g., people and funding); and
- Ensure accountability for performance.

This section presents an overview of the IT Sector's strategy and describes the process for developing protective programs that mitigate risk.

3.1 Current IT Sector Protective Programs

Table 3-1 describes protective program capabilities that support IT Sector goals. Additional information regarding existing protective programs, including a brief description of each, is provided in appendix 5. The list of protective programs in appendix 5 is not exhaustive. Rather, the programs are initial examples of sector protective programs (primarily federally sponsored) that address the sector's goals. Several protective programs encompass protective measures and activities that apply not only to the IT Sector but also to many other critical infrastructure sectors.

Value Proposition

The private sector's experience protecting, restoring, and reconstituting the IT infrastructure is a critical resource to the government in identifying future protective program needs, determining the overall effectiveness of protective programs to meet IT Sector goals, and implementing and/or participating in protective programs. The government provides resources and coordination for national-level programs. Whether protective programs are voluntary industry initiatives or national-level efforts sponsored by the Federal Government, the identification, development, and effective implementation of such programs facilitate risk management, situational awareness, and response, recovery, and reconstitution goals of the IT Sector.

Table 3-1: Protective Program Capabilities that Support IT Sector Goals

Goal	Outcome and Capability	Services Provided by Protective Programs
Prevention and Protection Through Risk Management	Vulnerability Reduction	A means to identify and obtain timely information on sector vulnerabilities; access to remediation and mitigation actions and best practices.
	Threat Analysis	An understanding of the threats facing the IT Sector and the Nation today and in the future.
	Modeling and Simulation	Capabilities to analyze and understand critical infrastructure interdependencies.
	High-Assurance Products and Services	Products and services with built-in security.
	Security Best Practices	Mechanism for identifying and sharing IT security best practices and protective measures.
Situational Awareness	Tactical Indications, Analysis and Warning	Information about incidents and other events as they are detected and unfold to raise awareness and understanding of the current operating environment.
	Information Sharing and Communications	A means for accessing and sharing information that enables decision makers to understand the current operating environment, form an opinion about the current state of security, and take action to respond to the events around them.
Response, Recovery, and Reconstitution	National Emergency Communications	Mechanisms to ensure that public and private sector security partners can communicate with one another during incidents.
	Incident Management and Incident Response Coordination	Capabilities to coordinate efforts to detect, contain, eradicate, and recover from incidents. Furthermore, analysis of lessons learned throughout each incident management life cycle phase enhances security partners' preparedness and prevention capabilities.
	Investigation and Attribution	Methods for attributing incidents to a person or persons with the ultimate goal of apprehending and prosecuting the suspected responsible parties.
	Contingency Planning/National-Level Planning	Actions that facilitate the exercise of plans, processes, and procedures to ensure individuals, organizations, the sector, and the Nation can respond and recover from incidents. Formal resource planning and allocation helps security partners identify needs for and uses of available mechanisms for coordination of materials and expertise to facilitate recovery.

Individual organizations also voluntarily implement protective initiatives and programs designed to enhance their physical, cyber, and human security. Taken together, these individual actions and measures enhance the overall security of the IT Sector. Examples of these actions include physical vulnerability mitigation measures (e.g., physical access control and surveillance), human vulnerability mitigation measures (e.g., employee screening and security training and awareness), cyber security measures (e.g., encryption), and business continuity planning. Such individual protective actions are outside the scope of this document.

3.2 Identification and Implementation of New Protective Programs

The following describes a process to determine the IT Sector's types of protective actions necessary to address priorities identified through the sector's risk management approach. This process will be used where individual entities cannot provide the mitigation, no viable private sector solution exists for meeting the need, or high transaction costs, legal barriers, or other impediments would cause significant coordination or implementation challenges.

3.2.1 Establish a Protective Program Working Group

An IT Sector Protective Program Working Group should be established to accomplish the following:

- Determine whether existing programs adequately promote the security of critical IT Sector functions;
- Identify any desired capabilities needed to address risk;
- Frame future protective program needs; and
- Make recommendations to the IT SCC and GCC for specific protective programs.

An effective Protective Program Working Group should include public and private sector representatives from entities such as the NCSD, IT SCC, IT GCC, and other security partners (e.g., representatives from other CI/KR sectors).

3.2.2 Determine Needs and Capabilities

The Protective Program Working Group will identify areas where protective measures are most needed to achieve the sector's goals. During the initial SSP development process, IT SCC and IT GCC members identified the following examples of capabilities that may be further considered in order to enhance the security of the IT Sector:

- **Robust Coordinated Response Capabilities.** The capability to respond to and recover from a nationally significant event is critical to promoting the resilience of the IT Sector and other CI/KR sectors. An all-hazards operational response and recovery capability is needed to bring public and private sector security partners together to coordinate activities. Emergency communications, collaboration, and analytical tools could enhance effective response; this may include bolstering existing public and private sector resources and capabilities.
- **Reconstitution of Data.** Data reconstitution tools and techniques are needed to ensure the integrity and availability of data. Development of a protective program should be linked closely to R&D activities designed to develop and pilot capabilities that enable key public and private sector systems to reconstitute rapidly data that could be corrupted, either intentionally or unintentionally.
- **Reconstitution of Communications Services and Networks.** A protective program initiative may be developed to assist with implementation of Federal Government authorities under Section 706 of the Communications Act applicable to key Internet functions. This program should also include developing the plans, programs, and mechanisms for identifying and refining requirements and developing reconstitution capabilities.

- **Out-of-Band Data Delivery Capability.** A protective program initiative is needed to provide mechanisms for delivering patches and other software to critical users if key Internet/network functions are not available. Such programs could include procuring space on satellites or unused television spectrum for moving software (e.g., critical patches or software) to key sites during a crisis or network congestion/failure.
- **Grants.** DHS should consider leveraging the existing grants process to more explicitly provide cyber security requirements for key State government operations that emphasize State activities, align them with Federal activities and the priorities described in the National Strategy to Secure Cyberspace, and enhance the States' operational cyber security.

The SSP development process also revealed that capabilities may be needed to facilitate the (1) development and demonstration of high-assurance products and services, (2) development and implementation of secure protocols, and (3) implementation of routine exercises and assessment of cyber security.

IT SCC and IT GCC members anticipate that additional needs and capabilities will be identified as the IT Sector's risk assessment approach is implemented. IT SCC and IT GCC efforts will provide the foundation for development of the IT Sector Annual Report, which will further define IT Sector protective program needs and priorities.

3.2.3 Identify Protective Actions

The Protective Program Working Group will identify protective activities to fulfill identified needs. The working group will consider the desired capabilities or outcomes that the program must achieve and the actions needed to provide those capabilities and outcomes. This effort will be linked closely with R&D efforts to ensure that activities for addressing desired capabilities are being developed and will be in the pipeline for implementation.

3.2.4 Develop an Implementation Plan

An initial implementation plan will be developed by the Protective Program Working Group for identified needs. The plan will include recommendations regarding the party or parties responsible for implementing the program, schedule, resources (e.g., facilities, budget, processes, and procedures), coordination with other programs, next steps, potential obstacles to success, and other considerations for successful initiation and maintenance of the program. Implementation of enhancements to existing programs or development of new protective programs may be filled by owners and operators, either voluntarily or based on various forms of incentives, or by cross-sector or national efforts undertaken by the Federal Government.

3.3 Protective Program Performance

Ongoing performance measurement will ensure that program performance aligns with intended IT Sector goals and will identify opportunities for continuous improvement. Federal departments and agencies, State and local governments, and organizations and associations that manage and oversee protective programs typically measure the performance of their programs just as owners and operators measure the performance of mitigation actions they use to enhance security.

Taking this into consideration, the IT SCC and IT GCC will meet annually to review overall progress toward IT Sector goals. During this annual meeting, IT SCC and IT GCC representatives will consider available information that reflects the progress of individual programs (e.g., Performance Assessment Rating Tool measures, program reviews), general views regarding needed capabilities, and the overall effectiveness of each protective program area. Review of individual programs will be left to those responsible for the program's implementation and maintenance. The IT Sector's approach to protective program performance and the review of overall progress follows the overall approach for tracking progress of IT SSP implementation as described in section 7.

3.4 Actions

The following bulleted list includes near term and long term actions to be completed to implement this section of the SSP.

3.4.1 Near Term (~1 year)

- Establish the joint IT SCC and IT GCC Protective Program Working Group to review existing protective programs, identify private sector programs, and refine and consolidate the list of current programs. (NCSD, SCC, and GCC)
- Hold annual meeting on protective programs before developing the IT Sector CI/KR Protection Annual Report. (NCSD, SCC, and GCC)

3.4.2 Long Term (1-3 years)

- Raise awareness of elected and appointed officials in all branches of State government of the IT Sector's role in CI/KR protection. (NCSD with SCC, GCC, and NASCIO input)
- Report on protective program successes and lessons learned in the IT Sector CI/KR Protection Annual Report. (NCSD with SCC and GCC input)
- Conduct joint discussions with the Communications Sector on protective program effectiveness and requirements for new protective programs to avoid duplication of efforts. (NCSD, SCC, GCC, NCS, Communications SCC, and Communications GCC)
- Manage protective programs sponsored by the Federal Government in close partnership with the private sector. (NCSD, GCC, and other Federal departments and agencies)



4. Information Sharing

Information sharing is a key element to fulfilling IT Sector goals and implementing the NIPP framework. Information sharing enables owners and operators, decision makers, managers, and others to detect, deter, and prevent attacks and incidents, identify trends, assess risks, provide warnings to help mitigate impacts, and coordinate response activities. Elements of information sharing include the following:

- Production of the information;
- Timely distribution of the information to specific, trusted partners and broader audiences; and
- Analysis and use of the information.

This section of the SSP describes the types of information that are important to IT Sector security partners and how that information is to be shared within the sector. This section also describes the following:

- Current IT Sector information sharing initiatives;
- Key focal points for policy and operational information sharing;
- Proposed process and procedural enhancements;
- Ways to provide greater access to information; and
- Near term (~1 year) and long term (1-3 years) actions to improve information sharing.

The ISAC Council Framework for Operational Information/Intelligence Sharing (Version 1.0, October 2006) provided a foundation for considering concepts and topics included in this section. The Council's framework provides a high-level set of components, which are part of an effective and manageable CI/KR protection information sharing infrastructure.²⁴

4.1 Types of Information

To be useful, information must be timely, relevant, actionable, and labeled so that recipients know the type of information and its sensitivity. The following descriptions of the categories of information that are produced, shared, and used by the IT Sector are consistent with information categories identified by the ISAC Council framework.

Value Proposition

Participation in the exchange of information among and between the public and private sectors provides a coordinated mechanism that will support the management of incidents, ultimately improving business continuity, continuity of operations, and resilience of IT Sector critical functions. Sharing timely and actionable information with security partners better enables them to prevent, protect, respond to, or recover from cyber or physical events, technological emergencies, or presidentially declared disasters that threaten, disrupt, or cripple IT Sector infrastructure.

²⁴ Additional information on the ISAC Council may be found at www.isaccouncil.org.

- **Analytical Product.** An analytical product contains the documented conclusions of public and private sector subject matter experts derived by applying threat information against known or perceived vulnerabilities to determine the likelihood of occurrence and the potential consequences. Analytical products include the following types of analysis:
 - **Tactical Analysis** examines factors associated with incidents under investigation or identified vulnerabilities to generate indications and warnings.
 - **Strategic Analysis** looks beyond individual incidents to consider broader sets of incidents or implications that may indicate threats of potential national importance. For example, strategic analysis may identify long-term threat and vulnerability trends that could provide advanced warnings of increasing risks, such as emerging attack methods. Strategic analysis gives decision makers information they can use to anticipate and prepare for attacks, thereby diminishing the potential damage. Strategic analysis also provides a foundation to identify patterns that can support indications and warnings.
- **Data.** Data include electronic, voice, or printed information routinely provided to trusted members for specified CI/KR protection purposes. Data products include the following types:
 - **Key Resources Data** is a list of assets and their locations (i.e., in the context of CI/KR protection, the building blocks of a critical infrastructure).
 - **Risk Data** pertain to information regarding the potential consequences to assets, functions, or services at risk, should the incident under study actually occur.
 - **Vulnerability Data** can be used to assess the degree to which given assets, functions, or services are vulnerable to the threat posed by the potential incident under study.
- **Incident Report.** An incident report should include details regarding the incident that has occurred, where it occurred, and when it occurred. The impact of the event will be reported as situational awareness.
- **Mitigation Actions.** Mitigation actions are operational practices that individual entities employ to enhance the security of their organizations. Examples include application of enterprise solutions to patch management, change management, configuration management, identity management, or procurement of secure systems. Entities may share information with one another or with other sectors regarding effective enterprise security practices.
- **Needs Requirement.** A needs requirement is any formal request for information (RFI) related to a threat, vulnerability, or incident.
- **Open Source Information.** Open source information is information available for non-restricted distribution.
- **Situational Awareness.** Situational awareness is an assessment of how an event affected specified assets and infrastructure, including consequential impacts on other infrastructures, missions, and functions. Situational awareness information includes the following:
 - **Advisories** are formal, narrative information bulletins intended to advise the recipient of certain facts, such as new threat information, the occurrence of an incident, or other information.
 - **Alerts** are indicators of a change in state. An alert is an advisory of an urgent nature. Alerts can be triggered for numerous reasons, including suspicious activity, aberrations or abnormalities detected during operations, or other information requiring increased awareness or attention from the sector. Although an advisory notifies and informs, an alert is a call to action.
 - **Threat Warning** provides information about an existing or developing threat that may lead to an incident. A warning is specific and actionable rather than merely stating a general concern about a potential event. A warning pertains to events that are imminent.

In addition to these information-sharing categories, information often has varying degrees of importance and uses. For example, shared information may be time sensitive, or it may be provided for long-term strategic use. Likewise, information may be of varying degrees of sensitivity, such as classified, unclassified, sensitive, proprietary, or open source. In addition, information often is disseminated in a tiered or phased approach based on disclosure constraints related to the sensitivity of the information.

4.2 Information Originators and Users

Public and private IT Sector security partners focus on building and maintaining trusted relationships to fulfill the IT Sector's goals based on the simple premise that, for information to be useful, it must be shared with the right people at the right time. This section focuses on sharing information between and among the government and those individuals who own, operate, and administer the IT infrastructure.

Information sharing often is done voluntarily. Private sector entities typically are not required or mandated to share information. In fact, private sector entities may even face Federal or State government limits on disclosure of sensitive information, and contractual obligations may restrict how and when information is disclosed. Information sharing within the public sector often is complicated by authorities and mandates governing information-sharing activities. For example, government may face difficulty sharing information because of its sensitivity (e.g., Privacy Act limitation on disclosure of personally identifiable information). Conversely, the government may be required to disclose information under the Freedom of Information Act (FOIA) or equivalent State disclosure laws.

A two-way flow exists between information originators and users. Information users are also information providers and vice versa. Each provides value to the information-sharing cycle. For example, entities that provide information determine how, when, and with whom to share the information and any restrictions that apply. Those who receive it determine how they will use it. Figure 4-1 describes the role of information originators and users.

Figure 4-1: Information Flows

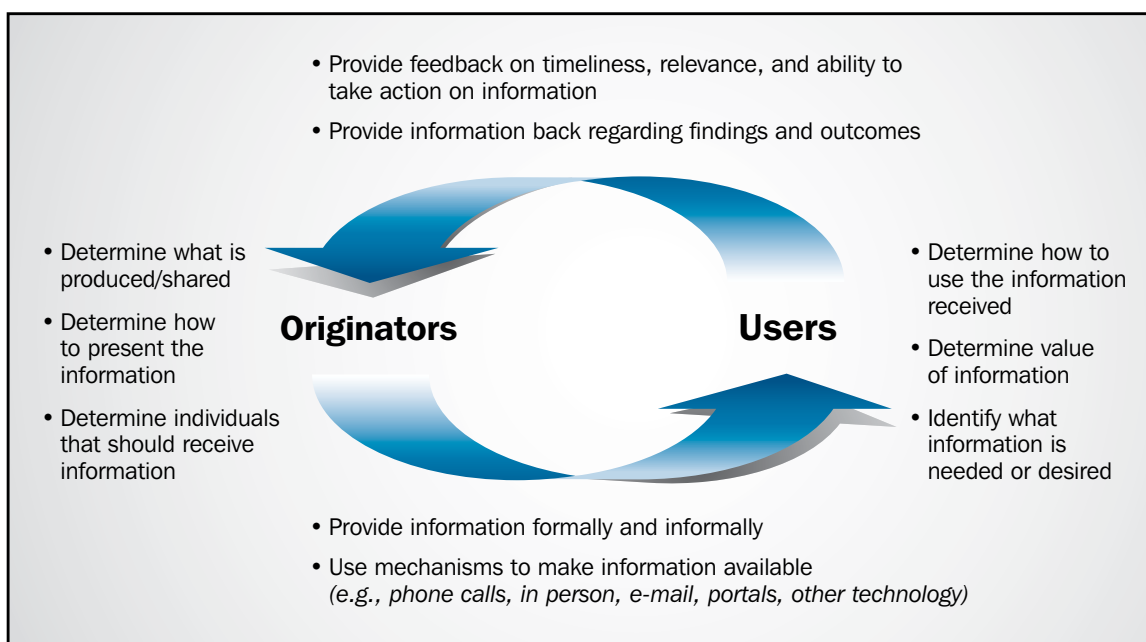
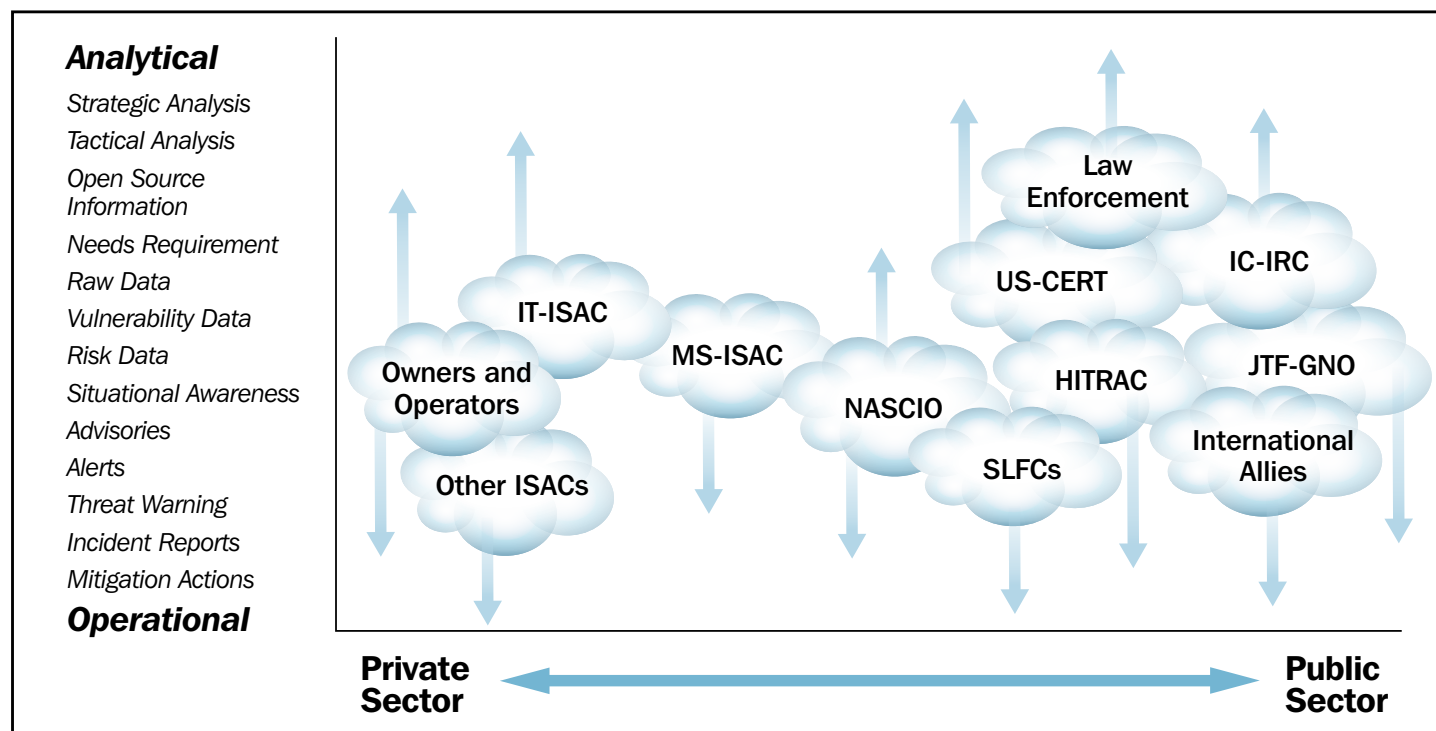


Table 4-1 provides a template for describing entities engaged in the information sharing cycle. It is a notional representation of a much larger and dynamic community of information sharing partners. Figure 4-2 illustrates the relationship between originators and users of the various types of information. The list of entities presented in Table 4-1 and Figure 4-2 are not all inclusive. Similarly, figure 4-2 only begins to describe the extent to which information is shared with others. Much additional work is needed to characterize and map who has the information, how it is shared, and with whom it should be shared. A near-term action to accomplish this effort is described in section 4.4.

Table 4-1: Types of Information Produced by Security Partners (Notional Template)

Information Originator	Category of Information											
	Analytical Products	Data: Raw Asset	Data: Risk	Data: Vulnerability	Incident Reports	Mitigation Actions	Needs Requirements	Open Source Information	Situational Awareness (SA)	SA: Advisories	SA: Alerts	SA: Threat Warning
IT-ISAC	X	X		X	X		X	X	X	X	X	
US-CERT	X	X	X	X	X	X	X	X	X	X	X	X
MS-ISAC	X	X		X	X		X	X	X	X	X	
Other ISACs	X	X		X	X		X	X	X	X	X	
NASCIO	X		X	X		X	X					
HITRAC	X								X			X
IC-IRC	X	X		X					X		X	X
JTF-GNO	X	X	X	X	X	X	X	X	X	X	X	X
NOC									X			
NICC	X				X		X		X		X	
Federal Law Enforcement Community	X				X	X		X	X	X	X	X
SLFCs	X						X	X	X			X
International –Allies	X	X	X	X	X	X	X	X	X	X	X	X

Figure 4-2: Notional Relationship Among Security Partners and Types of Information



4.3 An Enhanced IT Sector Information Sharing Framework

Implementing the IT Sector's vision for information sharing may require changes in policy, culture, organization, and technology to create the conditions that facilitate two-way, decentralized, coordinated, and trusted information sharing. Together, public and private sector entities and individuals can build an effective information-sharing environment that accomplishes the following:

- Facilitates the flow of information between and among public and private sector security partners in a timely, consistent, and predictable manner within a trusted environment, where information is received, disseminated, analyzed, and protected appropriately;
- Fosters a "need to share" culture, where incentives for sharing, especially for private sector entities, are realized clearly through value-added products and information;
- Identifies single points for coordinating information and assigns accountability, ensuring that information is being passed to the appropriate individuals;
- Establishes clear roles and responsibilities to help all security partners know how they fit into the information sharing landscape;
- Focuses on organizational levels, ensuring that established communication lines remain intact even when an individual leaves;
- Articulates incident reporting thresholds to define what constitutes an "incident" and ensures that a common baseline of corresponding actions exist for each level of severity;

- Creates uniform processes for protecting and disseminating information to ensure data are handled and distributed consistently across organizations and security partners to prevent unwanted disclosure; and
- Employs interoperable systems to enable users to communicate and exchange data efficiently across jurisdictional and organizational boundaries.

4.3.1 Information Sharing Focal Points

The IT Sector's vision related to focal points for information sharing is presented below:

- Institute an information sharing environment that ensures security partners can receive and disseminate information effectively and efficiently;
- Ensure that channels for building trusted relationships at the organizational level are institutionalized and considered routine practice;
- Obtain buy-in at the organizational level, ensuring that communications among partners are maintained regardless of personnel changes that take place within a company or government department or agency; and
- Ensure that security partners understand their respective roles, responsibilities, objectives, and incentives for sharing.

Achieving this vision requires designating organizations as focal points for gathering, analyzing, and disseminating information in a coordinated, reliable, and efficient manner. Defining these primary focal points and clarifying roles and responsibilities assigns accountability for accomplishing the IT Sector's vision for sharing information with the right people at the right time.

- **Current Initiatives:** The IT Sector has conduits for sharing information about policy issues and for sharing operational-level information. The primary conduits for policy issues are the IT SCC and IT GCC. The primary conduits for operational-level information exchange include the IT-ISAC for the private sector; the United States Computer Emergency Readiness Team (US-CERT); and the MS-ISAC for Federal, State, local, and international governments. Identification of key focal points for IT Sector information sharing enables the sector to maintain the flow of information and communication during contingencies.
- **Policy Mechanisms:** Consistent with the NIPP Base Plan, the IT SCC and IT GCC serve as the primary bodies for exchanging information on sector-wide policy issues pertinent to the IT Sector. As the strategic leadership for the IT Sector, representatives from both organizations work in close coordination to plan, develop, and coordinate sector-wide programs and initiatives, strategies, and policies. Other security partners play a role in policy-related information exchange and provide feeds into and use information generated by these two bodies. Through information exchange and collaboration, the IT SCC and IT GCC ensure that sector policies are coordinated and consistent with other national-level initiatives, other infrastructure sectors, SSAs, and other relevant parties, such as the PCIS and the Federal Senior Leadership Council, as needed.
- **Operational Mechanisms:** Consistent with the NIPP partnership model and fully endorsed by the IT SCC, the IT-ISAC is the IT Sector's focal point for coordinating the sharing and analysis of private sector information (operational and strategic) between and among members as well with other public and private security partners, including Federal, State, and local governments, international entities, and academic institutions. The IT-ISAC serves as a central repository for security-related information about threats, vulnerabilities, and best practices related to physical and cyber events, and is responsible for the receipt and dissemination of this information to ISAC members. The IT-ISAC also communicates with US-CERT and other sector-specific ISACs. Together, these capabilities offer members a current and coherent picture of the IT Sector's security.

US-CERT is a partnership between the DHS and the public and private sectors designed to facilitate protection of cyber infrastructure and to coordinate the prevention of and response to cyber attacks across the Nation. US-CERT is a 24/7 single point of contact (POC) for cyber analysis, warning, information sharing, and incident response and recovery for security partners, including the IT Sector. US-CERT interacts with Federal departments and agencies, including the IC (via the IC-IRC), the

private sector, academic and research community, State and local governments, the international community, and others to disseminate reasoned and actionable cyber security information to the public.

For State governments, the MS-ISAC serves as a focal point for information sharing with and among State and local governments. The MS-ISAC is a voluntary and collaborative organization with participation from all 50 States and the District of Columbia. It provides a common mechanism for raising the level of cyber security readiness and response in each State and with local governments. The MS-ISAC provides a central resource for gathering information on cyber threats to critical infrastructure from the States and providing two-way sharing of information. In addition, the DHS officially has recognized the MS-ISAC as the national center for the States to coordinate cyber readiness and response. The MS-ISAC and US-CERT exchange information regularly to facilitate national coordination of cyber security detection, prevention, and response activities.

The establishment of SLFCs across the Nation also provides a mechanism for the two-way flow of timely, accurate, actionable, all-hazard information between State and local governments and intelligence and law enforcement communities. SLFCs are multidisciplinary information-sharing hubs that bring together Federal, State, and local governments, law enforcement, and the private sector. During a regional or national event, SLFCs are intended to be central mechanisms for coordinating intelligence, resources, and situational awareness across the various levels of governments and with the private sector. Efforts to establish and operate SLFCs continue to evolve. Governance, staffing, funding, training, tools, processes, and technology are being identified, instituted, exercised, and maintained. As the capabilities and needs of the SLFCs mature, the IT SCC and IT GCC will define their relationship with the SLFCs.

4.3.2 Policies and Procedures for Sharing and Reporting Incidents

The IT Sector's vision for sharing and reporting incidents is provided below:

- Collect, disseminate, and share information along horizontal and vertical paths of an organization and among organizations;
- Communicate in a regular and predictable manner so that information is passed to all appropriate security partners and entities are not inadvertently omitted;
- Establish formal policies or procedures to prescribe the flow of information between and among public and private IT Sector security partners at all levels; and
- Develop formal triggers or incident-reporting thresholds to provide consistent guidance to owners and operators for determining when to elevate an event to a higher level or report it to the government.

Fulfilling this vision is critical to institutionalizing the timely and routine dissemination of information that fosters a culture of a "need to share" and minimizes duplication of effort.

Current Initiatives: The IT-ISAC has developed a template for organizations to use for sharing information with one another through the key focal points for IT Sector operational information sharing (i.e., IT-ISAC, US-CERT, and MS-ISAC). The structure for reporting information includes identifying the sender, target audience, use and/or type of information (e.g., general information, general action, analytical product, RFI, alert), sensitivity of the information, rules for disclosure, and timeliness of the information. Use of this template is supported by the IT-ISAC, the ISAC Council, and elements of DHS, including US-CERT. Broad acceptance across and use by private IT Sector security partners is desired.

4.3.3 Procedures for Protecting and Disseminating Sensitive Proprietary Industry Information

The IT Sector's vision regarding protecting and disseminating industry information is provided below:

- Work within an information-sharing environment that includes rules, policies, and procedures for protecting data to ensure that shared data are protected adequately and consistently across public and private sector organizations;

- Protect sensitive proprietary data from improper disclosure so that business integrity and public confidence are maintained and trust between and among public and private sector security partners is fostered; and
- Provide the appropriate operational and technical means to protect and secure data to ensure the integrity, availability, and confidentiality of the information.

Current Initiatives: The IT-ISAC and other information sharing organizations have implemented strict submission and classification guidance to protect sensitive proprietary data from unwanted disclosure. Membership in the IT-ISAC is dependent on adherence to these rules, which are enforced through contractual agreements. Members can submit information anonymously or with attributable, identifying information depending on their preferences or the sensitivity of the information. They also may label submissions designating who can view the information (e.g., the public, IT-ISAC membership, or only the ISAC for trending and analysis purposes). Submitted information is protected appropriately according to labeling requirements. Memorandums of understanding (MOUs) with partners and a consistent labeling framework help ensure that rules and procedures for sharing information are followed. For example, MOUs with other sector ISACs facilitate the exchange of threat and vulnerability data across sectors. This information is vital to assessing IT Sector risk and also helps other infrastructure sectors understand risks posed by vulnerabilities in the IT Sector.

Protected Critical Infrastructure Information (PCII) Program: To protect information that is voluntarily shared with the Federal Government, Congress passed the Critical Infrastructure Information Act of 2002 (CII Act), Subtitle B, of the Homeland Security Act of 2002, Public Law 107-296. The CII Act's purpose is to encourage the private sector to voluntarily submit CII, which often contains proprietary and confidential information, to the DHS by protecting CII from disclosure under FOIA and State and local government open records laws, and from use in civil litigation. The CII Act authorizes the DHS to receive voluntarily submitted information that qualifies for protection and to give it special protection as specified by the CII Act. In accordance with the act, the DHS established the PCII Program to encourage infrastructure owners and operators to share sensitive information voluntarily.

The PCII Program Office receives, evaluates, stores, and shares voluntarily submitted information that qualifies for protection under the legislation. Submissions under the program may be used for various homeland security purposes, including analyzing sector risk and vulnerabilities, securing and protecting systems, and informing response and recovery efforts. PCII is shared with Federal, State, and local governments that are certified to handle PCII and provides a feed into tactical and strategic analysis, vulnerability assessments, alerts, and other products that are shared with various audiences. Federal departments and agencies and State and local governments are among those that have been certified to handle PCII and are using the program to facilitate the sharing of information. The PCII Program also provides a single submission entity to reduce duplicative requests for information. Despite the establishment of the PCII Program, many private infrastructure owners and operators remain hesitant to share information and are unsure about the department's ability to protect their information. In addition, the benefits to the private sector of sharing sensitive information have not been articulated clearly, although the associated risks are clear.

4.3.4 Access to Classified and Sensitive But Unclassified (SBU) Government Information

The IT Sector's vision for sharing classified and SBU government information is provided below:

- Ensure that all key partners, including State and local government officials and private industry personnel, have the requisite clearances for obtaining access to pertinent threat data and analyses provided by the IC;
- Promote uniform policies and procedures governing the designation, handling, and distribution of sensitive data such as law enforcement sensitive (LES), for official use only (FOUO), and SBU data; and
- To foster trust by ensuring uniformity and consistency in the level of protection afforded and rules or circumstances for further dissemination, which both help to minimize the risk of compromise and improper disclosure.

Current Initiatives: Security clearances and classifying data enable the Federal Government to protect and restrict access to sensitive or classified information to those with requisite background investigations and a demonstrated need to know. Strict handling and dissemination rules for classified data ensure appropriate and consistent protection and dissemination of that data. Federal departments and agencies have been working with the IT SCC and State and local government officials to grant security clearances to private sector and State and local government officials. The Federal Government, in particular the IC, has been working to develop regular processes for sanitization and production of classified information in a way that allows it to be shared, even if it comes from sensitive methods and sources (e.g., tear-line reports). For example, HITRAC is developing and providing periodic classified threat briefings and reports to appropriately cleared IT Sector security partners and other infrastructure sectors.

4.3.5 Mechanisms for Communicating and Disseminating Information

The IT Sector's vision for information communication and dissemination mechanisms is provided below:

- Ensure automated communication tools can send broadcast messages or alerts to a defined community of users, provide forums for the exchange of information on vulnerabilities, and raise awareness of security issues; and
- Have access to and use of tools for information exchange—whether voice, data, and network based—that are secure, robust, survivable, and interoperable.

Current Initiatives: Technology is a key enabler for effective information sharing. It provides security partners the means to share and exchange various types of data in real time and across jurisdictional and organizational boundaries, enabling key partners to work from a common understanding of the situation. IT Sector security partners use various communications tools to exchange information with each other and with other sectors. These tools facilitate the exchange of information between individuals and larger communities or audiences as needed.

Regular meetings and conference calls also provide a mechanism for exchanging various types of information. The IT-ISAC's Technical Committee exchanges information internally through twice-a-week conference calls, a secure Web site, and encrypted e-mails. The IT-ISAC maintains a Web site for sharing information with the public and internally with its members. A secure portion of its Web site is reserved for ISAC member companies to share information with one other. In addition, the IT-ISAC hosts a daily cyber conference call with US-CERT and the operations centers of other ISACs, as well as a weekly conference call focusing on physical issues with only the operations centers of other ISACs. The Department of Defense (DOD) and the IC also host numerous conference calls and video teleconferences to share information daily.

In addition, other tools provide a means for communicating and exchanging information during crises or emergencies, including programs such as the Critical Infrastructure Warning Information Network (CWIN), Government Emergency Telecommunications Service (GETS), Wireless Priority Service (WPS), and ENS Appendix 4, Protective Programs, provides additional detail about these programs.

4.4 Actions

The following bulleted list includes near term and long term actions to be completed to implement this section of the SSP.

4.4.1 Near Term (~1 year)

Focal Points for Information Sharing

- Coordinate and integrate IT-ISAC and IT SCC efforts by offering recipient IT-ISAC membership to all IT SCC members and defining the roles and responsibilities of each organization to coordinate initiatives more effectively, assign accountability, and minimize duplicative efforts. (IT-ISAC and SCC)

- Increase the IT-ISAC's reach by augmenting current recruitment efforts by instituting a partnership program whereby ISAC membership is offered to representatives of IT trade associations and other IT-related organizations. (IT-ISAC and SCC)
- Identify and share POC lists to improve the ability to draw on the subject matter expertise available throughout the sector and to interact and coordinate with law enforcement for routine preparedness activities, as well as crisis situations requiring continuity of operations and continuity of government activities. (SCC, IT-ISAC, GCC, NCSD)
- Exchange information with the Communications SCC and coordinate on issues related to convergence of the IT and telecommunications infrastructures. Designating an IT SCC representative to serve on the Communications SCC and including a Communications SCC representative on the IT SCC Executive Committee will facilitate the exchange of information. (SCC)

Policies and Procedures for Sharing and Reporting Incidents

- Work with State and local governments to refine the security focus of SLFCs and clarify the relationship between SLFCs and the private sector, including clarifying how SLFCs relate to other information-sharing mechanisms sponsored by DHS and how information flows between entities. (DHS and NCSD with input from SCC and GCC)
- Develop a Concept of Operations (ConOps) to formalize information sharing within the IT-ISAC's membership and between the IT-ISAC and external organizations, including US-CERT. (IT-ISAC) (Underway)
- Develop a Private Sector ConOps to guide US-CERT interaction with the private sector. (US-CERT with input from the ISAC community and other private sector security partners) (Underway)
- Develop MOUs to establish, where appropriate and necessary, formal information-sharing agreements at the organizational level to better facilitate data exchange. (Individual GCC and SCC entities or other security partners as appropriate)

Procedures for Protecting and Disseminating Sensitive Proprietary Industry Information

- Raise awareness about the PCII Program among Federal, State, and local government and private sector participants and articulate the value that participants in the PCII Program can derive from submitting sensitive information. (DHS PCII Program)
- Assess the use of the PCII Program for submitting sensitive information, including risk management information, to the government. (SCC, other private sector entities, GCC, and State and local governments)

Access to Classified and SBU Government Information

- Identify private sector security partners with Federal Government-issued security clearances that should receive government information, and provide their names and pertinent contact information to the DHS and other Federal departments and agencies (e.g., the IC-IRC) to facilitate more timely and extensive sharing of critical and actionable classified intelligence information with appropriately cleared individuals and organizations. (SCC, IT-ISAC, and NCSD)
- Identify mechanisms for private sector and State and local government officials who have security clearances to gain access to classified information pertinent to the IT Sector. (DHS with input from NCSD and NASCIO)

Mechanisms for Communicating and Disseminating Information

- Identify, update, and maintain appropriate private sector and State and local government POCs who should participate in emergency communication mechanisms such as CWIN, ENS, GETS, and WPS. (NCSD and NCS with SCC, IT-ISAC, and NASCIO input)
- Routinely test and exercise processes, procedures, emergency communications systems, and capabilities; document lessons learned; and make recommendations for improvement. (NCS with NCSD, SCC, and GCC input)

- Use Homeland Security Information Network for Critical Sectors (HSIN-CS) as a mechanism for exchanging information with IT Sector private sector security partners. As information is made available, the IT-ISAC will pull it from HSIN-CS and push it to IT-ISAC members for their use. (NCSD and other components of DHS, IT-ISAC)
- Adopt a common format (e.g., ISAC council template) for presenting information that is shared with the IT Sector private sector security partners. (NCSD working with other components of the DHS)
- Develop a strategy to leverage the Homeland Security Information Network (HSIN) to exchange IT Sector information with State and local governments. The strategy may consider duplicating or leveraging the IT-ISAC process of pulling information from HSIN-CS and pushing it to IT-ISAC members. (NCSD and other components of the DHS with NASCIO input)

4.4.2 Long Term (1-3 years)

Focal Points for Information Sharing

- Encourage public and private sector security partners to commit to participating in the NIPP partnership model, specifically the ISACs, including the IT-ISAC and MS-ISAC. (DHS Office of Infrastructure Protection (OIP), NCSD, NCS, and other DHS components)
- Address areas of convergence, such as those identified in the President's National Security Telecommunications Advisory Committee (NSTAC), NSTAC Report to the President on the National Coordinating Center,²⁵ including developing an approach for a long-term regional communications and IT coordinating capability that serves all regions of the Nation, convening a conference to focus on cyber issues, and exploring ideas for a multi-industry coordinating center. (NCSD, NCS, GCC, SCC, Communications SCC, and Communications GCC)

Policies and Procedures for Sharing and Reporting Incidents

- Undertake an initiative to characterize and map the flow of information between and among security partners for all stages of preparedness activities. This initiative should include information on who shares what information, who receives the information, and what networks and systems are being used to disseminate and exchange the information. (NCSD and other DHS components with input from SCC, IT-ISAC, and GCC)

Procedures for Protecting and Disseminating Sensitive Proprietary Industry Information

- Develop the mechanisms and capabilities (e.g., access controls, user rights, and authentication) needed to assure the private sector that its data will be protected. (NCSD and other DHS components with input from SCC, IT-ISAC, and GCC)
- Familiarize government entities with IT-ISAC tiered information-sharing mechanisms and capabilities. (NCSD and IT-ISAC)

Access to Classified and SBU Government Information

- Explore ways of clarifying the procedures for handling FOUO, SBU, LES, and other sensitive information. (Homeland Security Council with input from NCSD, SCC, and GCC)

Mechanisms for Communicating and Disseminating Information

- Design, develop, and implement a protected information-sharing architecture as outlined in the NIPP. (DHS Office of Infrastructure Protection, Information Sharing Environment)
- Exercise processes and procedures (e.g., standard operating procedures and ConOps) and communication mechanisms (e.g., HSIN-CS, GETS, CWIN, and WPS) and evaluate lessons learned to enhance information sharing from a cultural, organizational, and technological perspective. (NCSD, NCS, DHS Office of Infrastructure Protection, SCC, GCC)

²⁵ President's National Security Telecommunications Advisory Committee (NSTAC), NSTAC Report to the President on the National Coordinating Center, May 10, 2006.

Achieving an enhanced information-sharing framework requires commitment from public and private sector security partners. Participation in the IT SCC and IT GCC requires commitment not only on the part of individual members, but also on the part of the organizations employing them. Implementation of the above actions cannot be achieved without a core group of committed individuals from the public and private sectors. This core group of individuals and organizations may not necessarily be the same as those who were responsible for outlining the vision for an enhanced information-sharing framework. Investment in resources and human capital is necessary for success.

5. CI/KR Protection Research and Development

Over the past several years, several committees and organizations have analyzed and reported on IT Sector security gaps. The result is a substantial body of work describing these gaps and proposing R&D priorities to bridge them. Although each of these analyses is a call to action for a unique audience, the underlying themes, overall conclusions, and resulting objectives are consistent across the board. This section leverages this work to build a structure for IT Sector R&D based on the common themes established by these prior analyses.

Value Proposition

Visibility into R&D priorities and initiatives being undertaken by the private sector and Government break down existing barriers and promote collaboration to ensure that resources are allocated and used efficiently, R&D initiatives are timely, and ultimately products and services are in the pipeline in time to enhance the security of the IT Sector and the Nation.

5.1 Current IT Sector Research and Development

This section describes existing analytical work, identifies common themes among them, and documents new areas of importance not covered previously. The President's Information Technology Advisory Committee's (PITAC) *Cyber Security: A Crisis of Prioritization* (February 2005) and the National Science and Technology Council's (NSTC) *Federal Plan for Cyber Security and Information Assurance R&D* (April 2006) provide a foundation for this section because they are timely and represent two ends of a spectrum in terms of granularity and depth of discussion. In addition, these two reports represent the points of view of private sector experts and the Federal Government. These reports not only convey the thoughts of the authors themselves but also are compilations of the many other previous reports that the authors used to construct their analyses. For example, the PITAC analyzed more than 30 reports to develop its conclusions and 10 areas of prioritization. In addition to these primary references, this section builds on concepts from the following documents to construct the common themes:

- Internet Architecture Board (IAB) Concerns and Recommendations Regarding Internet Research and Evolution, Internet Engineering Task Force, Request for Comments 3869, August 2004
- Grand Research Challenges in Information Security and Assurance, Computing Research Association, November 2003
- The National Strategy to Secure Cyberspace, The White House, February 2003
- The Cyber-Posture of the National Information Infrastructure, RAND Corporation, 1998
- National Cyber Security Research and Development Act (Public Law 107-305), 2002
- Hard Problems List, INFOSEC Research Council, 2005

- The National Plan for R&D in Support of CIP, Office of Science and Technology Policy (OSTP), Executive Office of the President, and Science and Technology (S&T) Directorate, DHS, 2004

Following are the common prioritization themes reflected in these analyses:

- Cyber situational awareness and response;
- Forensics;
- Identity management: authentication, authorization, and accounting;
- Intrinsic infrastructure protocols security;
- Non-technology security issues;
- Control systems security;
- Scalable and composable secure systems;
- Secure coding and software engineering; and
- Trust and privacy.

5.2 IT Sector R&D Priorities

This section presents the IT Sector R&D priorities, which often are consistent with existing studies. However, additional items are included to align these priorities with the overall IT Sector goals. Some of the following factors have influenced this work:

- Greater involvement of the private sector envisioned in the R&D efforts;
- Greater focus of the SSP on elements that can be executed quickly and effectively; and
- SSP time horizon of 1-3 years in terms of completing research projects, or beginning them, even if the eventual delivery horizon is longer.

The IT SCC and IT GCC identified the following IT R&D priorities listed alphabetically:

- **Cyber Situational Awareness and Response.** Research into development of tools and techniques allowing for greater awareness of the state of an IT environment resulting in a timely public and private sector response to factors affecting its security.²⁶
- **Forensics.** Research into mechanisms for identifying, tracking, and bringing to justice perpetrators of crimes leveraging cyberspace.²⁷
- **Identity Management: Authentication, Authorization, and Accounting.** Research into scalable, user-friendly mechanisms for ensuring access to resources based on the identity of the requestor.²⁸
- **Intrinsic Infrastructure Protocols Security.** Research on building security into foundational protocols, such as the DNS, Border Gateway Protocol (BGP), Session Initiation Protocol (SIP), and others on which the information infrastructure is built. This effort includes research toward fundamentally improving the security of relatively new IT technologies, such as wireless and Voice over Internet Protocol (VoIP).²⁹

²⁶ Sections 1.4, 1.5, 1.6, 1.7 and 1.8 of NSTC plan, Functional Cyber Security; sections 5 and 6 of PITAC report, *Monitoring and Detection and Mitigation and Recovery Methodologies*.

²⁷ Section 1.9 of NSTC plan, Forensics, Trace Back and Attribution; section 4 of PITAC report, *Cyber Forensics: Catching Criminals and Deterring Criminal Activities*.

²⁸ Section 1.1 of NSTC plan, Authentication, Authorization, and Trust Management; section 4 of PITAC report, *Authentication Technologies*.

²⁹ Sections 2 and 3 of NSTC plan, Securing the infrastructure and Domain Specific Security; section 4 of PITAC report, *Secure Fundamental Protocols*.

- **Modeling and Testing.** Research on building scalable tools and test beds to develop a greater understanding of the state of currently deployed technologies, as well as the readiness of technologies about to be deployed in the field.³⁰
- **Control Systems Security.** Research into improving the security of process control systems and associated information networks that cut across almost all critical segments of society.³¹
- **Scalable and Composable Secure Systems.** Research into the security of larger systems formed by integrating smaller systems to achieve various scalability objectives.³²
- **Secure Coding, Software Engineering, and Hardware Design Improvement.** Research into improving the way software and hardware are developed to meet needs for reducing vulnerabilities resulting from software and hardware flaws.³³ Technology life cycle assurance mechanisms, including advanced engineering disciplines, standards and certification regimes, and best practices are important to this work. Research areas to focus on include investigation into refining current assurance mechanisms and developing new ones where necessary, developing certification regimes and exploring policy and incentive options. All of these must be provable in terms of demonstrating a reduction in security issues.
- **Trust and Privacy.** Research into ways to ensure that IT systems protect the privacy rights of individuals using IT systems while maintaining overall system security.³⁴

5.3 Coordinating IT Sector R&D Priorities

The IT SCC and IT GCC will facilitate awareness and, where possible, coordination of IT security research. The IT GCC is a source of Federal Government expertise and can provide access to individuals and programs responsible for identifying research priorities and managing their implementation. Such facilitation requires engaging multiple partners in the R&D process to pool resources toward the objective of awareness and coordination.

To initiate this process, the IT SCC and IT GCC will establish an R&D Working Group that will engage with research-oriented partner organizations to help implement the proposed initiatives described in this section (see text box), and others as they evolve. The following list includes possible security partners but is not exhaustive; additional entities may be identified as the R&D efforts evolve.

Relevant Federal Government bodies include the following:

- OSTP;
- DHS S&T Directorate;
- Defense Advanced Research Projects Agency;
- National Science Foundation (NSF);
- NIST;
- Naval Research Laboratory;
- President's Committee of Advisors on Science and Technology;

³⁰ Section 6 of NSTC plan, Enabling Technologies for Cyber Security and Information Assurance R&D; section 8 of PITAC report, *Modeling and Test Beds for New Technologies*.

³¹ Section 2.4 of NSTC plan, Secure Process Control Systems.

³² Section 7.3 of NSTC plan, Composable and Scalable Secure Systems.

³³ Section 5.x of NSTC plan, Foundations for Cyber Security; section 4 of PITAC Report, *Secure Software Engineering and Software Assurance*.

³⁴ Section 8.x of NSTC plan, Social Dimensions of Cyber Security; section 10 of PITAC report, *Non-Technology Issues That Can Compromise Cyber Security*.

- Interagency Committee on Networking and Information Technology Research and Development;
- National Research Council;
- NSTC;
- U.S. House of Representatives Committee on Science; and
- U.S. Senate Committee on Commerce, Science and Transportation.

Private sector associations include the following:

- Computing Research Association;
- Association of Computing Machinery; and
- Internet2.

Two potential mechanisms for further coordinating IT Sector security research include the establishment of an online clearinghouse for exchanging information and collaborating on IT Sector R&D priorities and conducting an annual IT Sector R&D workshop to provide a means for conducting outreach, reviewing research projects in the pipeline, considering shortfalls in the execution of national research priorities, and reaching consensus on general requirements for government and private sector funding and human resource requirements for ongoing and new research initiatives.

In addition, a common taxonomy for exchanging information on progress toward accomplishing the IT Sector's goals for each R&D priority area can promote an understanding across the IT Sector R&D community and further collaboration activities. The following questions can form the foundation for a common taxonomy:

- **How many projects are underway in pursuit of that priority?** Although quantity is not a comprehensive measure of success, it is important to track the various efforts focused on a given objective.
- **What is the relevance of each project to the goal of the area, and to what extent does each project solve the problem the area identifies?** It is conceivable that some projects would be more relevant than others. It is important to track the relevance of the projects to measure how they affect the desired outcome.
- **What is the potential for each project to result in products that can be transitioned to the field?** This is a test of the project's ability to provide practical solutions.

Potential Coordination Mechanisms

Online Clearinghouse. Establish and maintain a searchable clearinghouse that accomplishes the following:

- Enables individuals and organizations interested in R&D efforts to quickly and easily gauge the state of the art in a particular area of interest;
- Stimulates cross-pollination of ideas from one area of work to another within the IT Sector and between the IT Sector and other sectors;
- Facilitates collaboration within and between public and private sector entities while leveraging their collective efforts and resources; and
- Describes research projects in a common format, and develops and implements processes for gathering, organizing, and maintaining relevant data online.

Projects should be categorized at a high level based on IT Sector R&D priorities. The overall aim would be to provide visibility to public, private, and academic IT security research projects. It is envisioned that current solutions together with enhancements and new developments could provide the foundation for such an online clearinghouse.

Annual IT Sector R&D Workshop. A joint IT SCC and IT GCC annual IT Sector R&D workshop can provide:

- An ongoing mechanism for the IT Sector to gauge the work being done against the priorities it has established;
- A forum where R&D priorities can be discussed and updated by individuals involved in R&D work in various capacities;
- A mechanism to bring private sector and Government together to address common priorities and collaborate on R&D efforts; and
- A forum to highlight and acknowledge the most important work undertaken over the past year toward achieving R&D priorities.

- **At what stage of completion is each project?** This is a measure of the current progress toward achieving the goals of the research area.

It will be important for the government to leverage resources in the private sector to achieve the R&D goals that it shares with the private sector. Leveraging private sector R&D investment while respecting the proprietary nature of some of those efforts is critical to the overall strategy. Demonstrating a value proposition that will motivate the continued and expanded participation of the private sector is a fundamental tenet of the overall SSP process.

5.4 Actions

The following bulleted list includes near term and long term actions to be completed to implement this section of the SSP.

5.4.1 Near Term (~1 year)

- Establish an IT Sector R&D Working Group and identify opportunities for public and private sector security partners to collaborate on R&D priorities. (NCSD, S&T Directorate, SCC, and GCC)
- Brief R&D institutions listed above on the SSP to raise awareness of IT Sector R&D priorities, goals and objectives, and risk management approach. (NCSD, S&T Directorate, SCC, GCC)
- Coordinate with the Communications Sector on R&D CI/KR protection priorities that overlap or have inherent synergies. (NCSD, SCC, GCC, NCS, Communications SCC, and Communications GCC)

5.4.2 Long Term (1-3 years)

- Plan and execute annual IT Sector R&D Workshop and share results with R&D public and private sector security partners. (SCC and GCC)
- Develop a 5-year roadmap for IT Sector R&D priorities and resource needs. (S&T Directorate and NCSD with input from SCC and GCC)



6. Managing and Coordinating Sector Responsibilities

This section addresses the IT Sector’s overall approach for managing and coordinating Sector responsibilities.

6.1 Program Management Approach

HSPD-7 designated the DHS with responsibility for managing and coordinating IT Sector CI/KR protection activities, including leading the development, implementation, and maintenance of the SSP in coordination with the IT SCC and IT GCC. This responsibility has been delegated to NCSD within the DHS’s Office of Cyber Security and Communications.

Value Proposition

Developing collaborative and coordinated roles and responsibilities for managing IT Sector CI/KR protection activities provides the foundation for open channels of communication among government and the private sector for implementation of the SSP.

6.2 Processes and Responsibilities

The following sections outline IT Sector processes and responsibilities.

6.2.1 SSP Maintenance and Update

The IT SSP is a living document; consequently, NCSD, IT SCC, and IT GCC representatives will review and update it annually to reflect changes in the sector’s security posture and programs. This annual update will leverage the partnership between the IT SCC and IT GCC in developing this plan and will build on the processes used to develop this plan. For example, the IT Sector Plans Working Group will continue to facilitate discussions and dialogue regarding the IT SSP.

The NIPP also will be reviewed triennially by the DHS. NCSD will work closely with the IT SCC, IT GCC, and other security partners to coordinate their participation in the triennial review. Any changes in the NIPP based on the triennial review will be incorporated in the IT SSP annual update.

6.2.2 Annual Reporting

HSPD-7 mandates that each sector shall produce Sector CI/KR Protection Annual Reports to identify, prioritize, and coordinate CI/KR protection in its sector. The NIPP Base Plan provides additional details about these reports. The reports are to be submitted to DHS on July 1 of each year and will describe the sector’s CI/KR protection goals, priorities, programs, and related funding, as well as report on progress in the area of CI/KR protection. NCSD will develop the IT Sector CI/KR Protection Annual Report and seek input from the IT SCC and IT GCC to ensure that it accurately reflects the range of sector activities.

6.2.3 Resources and Budgets

Ability to achieve the actions in this plan is dependent on the availability and allocation of resources. Public and private IT Sector security partners make investments and contribute resources (e.g., people, time, and money) to operate critical IT Sector functions and promote the resilience and security of those functions. Because of the sector's diversity and the number of security partners providing resources to secure the sector, neither NCSD nor any other entity has authority over resources and budgets for the entire sector. The NIPP process is designed to prioritize programs and R&D efforts to ensure funding flows to the most critical areas of the IT Sector. The IT GCC and IT SCC will work together to ensure that public and private sector spending reflects the best allocation of available resources.

Managing Sector Resources

IT infrastructure owners and operators ultimately manage their own resources in securing their respective portions of the IT Sector's infrastructure. Federal, State, and local government also manage resources to ensure the availability and resilience of government services. NCSD is responsible for managing some of the Federal Government's resources that support the CI/KR protection of the sector. NCSD will work with other Federal departments and agencies, through the IT GCC, to coordinate priorities for non-SSA funding and resources that support the sector. The private sector can aid in resource allocation decisions by helping the government better understand the resource impact of CI/KR protection and security demands made on the sector and the trickle-down effect on citizens and consumers. Understanding what levels of security investment exceed enterprise capability can help NCSD justify the allocation of resources for national-level capabilities and programs that contribute to the resilience of critical IT Sector functions.

Investment Priorities

Through the IT Sector CI/KR Protection Annual Report, NCSD will identify investment priorities based on risk management priorities, lessons learned, the success of protective programs, and identified needs. NCSD will compile this report in coordination with public and private sector security partners. The report will include priorities and program funding for the current year and projected funding for the following year.

Federal Funding

The annual Federal funding cycle is described below:

- **February Through June:** NCSD coordinates with other DHS components to develop recommendations concerning the DHS budget requests. This request includes funding for IT Sector security-related expenditures that are supported by NCSD and the DHS.
- **September 1:** NCSD submits its budget requests for the following fiscal year.
- **September Through November:** NCSD, through DHS headquarters, works with OMB to make final decisions regarding the DHS budget and resources available for the division and specific IT Sector programs.

6.2.4 Training and Education

Training and education are crucial to maintaining individual and organizational CI/KR protection expertise and to implementing the risk management framework successfully. Rapid changes in technology (e.g., the growth of e-learning) affect how training is delivered and what competencies are needed (e.g., the growing need for information security skills). An important component of a comprehensive IT security workforce development program is the enhancement and professionalization of the individuals currently involved in IT security operations and program management. A recently completed study estimated that there are 1.5 million information security professionals throughout the world.³⁵ Of this total, approximately 40 percent are employed in the U.S. and Canada. IT security has become a separate and distinct career field. The continuing education and

³⁵ Allan Carey, IDC White Paper: 2006 Global Information Security Workforce Study, October 2006.

development of the current IT security workforce is an important aspect of the initiative to improve the security posture of the nation's IT infrastructure.

- **National Centers of Academic Excellence in Information Assurance Education (CAEIAE).** The CAEIAE program, founded in 1998 by the National Security Agency (NSA), has been co-sponsored by DHS since 2004. The program is open to 4-year colleges and universities that demonstrate significant depth and maturity in their information assurance (IA) programs. CAEIAEs must map portions of their security curricula to at least two IA standards from the Committee on National Security Systems. The schools may reapply every 3 years to be redesignated as CAEIAEs. As of December 2006, 75 schools in 32 States and the District of Columbia are designated. The CAEIAE program plans to have at least one center in every State.
- **Federal Cyber Service: Scholarship For Service (SFS).** The SFS program, originally established by NSF in 2001, has been co-sponsored by DHS since 2004. This program provides scholarship money for a maximum of 2 years to outstanding cyber security undergraduate, graduate, and doctoral students in exchange for an equal amount of time spent in Federal Government service after graduation. Eligible students must attend a university or college designated as a CAEIAE. As of December 2006, 30 institutions are participating in the SFS program.
- **Project MBA.** NCSD and DHS's Risk Management Division (RMD) launched Project MBA in January 2006 as an effort to incorporate elements of physical and cyber security in business school curricula. The pilot program, which takes place at George Mason University's School of Management, includes simulations, lectures, and discussions on topics such as emergency preparedness, business continuity planning, and cyber security. Based on feedback from the pilot, the program may be expanded to additional graduate business schools during the 2007 academic year.
- **Professional Certifications.** Professional certifications have become recognized as an important qualification for individuals who chose IT security as their career field. Over the past ten years the number of individuals attaining a professional IT security certification has grown dramatically. This growth reflects not only the rapid increase of individuals entering the IT security field, but also growth in the number and diversity of available certifications. These now range from highly technical, vendor specific credentials to those which cover the broad spectrum of information security in a product neutral manner.
- **Department of Defense IT Security Workforce Enhancement Program.** The Department of Defense (DOD) has recognized that a critical factor in improving the security of their information systems infrastructure is the development of a skilled, professional IT security workforce. DOD has established a fundamental requirement that all employees (i.e., active duty and reserve military, civilian personnel—to include foreign nationals, and contractors) who have privileged access to a DOD system, or are involved in security management, must attain professional certification by the end of fiscal year 2010. The Department estimates that this requirement will apply to approximately 100,000 individuals. DOD has approved various "commercial" certifications as meeting their requirements in both the managerial and technical tracks.
- **Other Professional Development Activities.** As the IT security profession matures, there is growing recognition of the need to maintain and enhance their technical and managerial skills. Numerous conferences and educational events are held each year that cover various aspects of the IT security problem. These provide an opportunity for individuals in the public and private sectors to exchange information in a collaborative environment. In addition, there has been a growth in professional associations that provide educational forums, publications and peer interaction opportunities that enhance the knowledge, skill and professional growth of their members.
- **Exercises.** Tabletop and full-scale exercises fulfill many training and education objectives. In addition to supporting specialized training for individuals, exercises support cross-sector training, as well as general outreach and awareness. For example, NCSD sponsors the National Cyber Exercise (Cyber Storm) series, which strengthens preparedness, response, coordination, and recovery mechanisms within Federal, State, and local governments, and in conjunction with the private sector. In accordance with congressional mandates to conduct exercises that test response to cyber attacks on critical infrastructures, the exercise meets HSPD-8, National Preparedness, requirements. It is coordinated with the DHS National Exercise Program.

The National Cyber Exercises provide the venue for the DHS; the SSAs; other Federal agencies; the private sector; and State, local, and tribal government entities to identify interdependencies, integrate infrastructure protection activities within other national-level plans, identify overlaps, rectify gaps, and establish mechanisms for coordination and information exchange. The National Cyber Exercise sponsors collaborate with various security partners throughout the coordination, planning, and execution of an exercise. The private sector is one of the most significant security partners for the National Cyber Exercises. Because the private sector owns or operates more than 85 percent of the critical infrastructure, its involvement in the planning process and execution of any CI/KR exercise is inherently crucial to its success. NCSD works closely with the IT SCC and IT-ISAC to facilitate and promote private sector involvement in its exercises.

- **Future Plans and Initiatives.** Training and education is a continuous process and is a responsibility of the public and private sectors. Future CI/KR protection training and education efforts are focused on aligning training programs with IT Sector goals and objectives; identifying and assessing standard training needs for the entire sector; allocating training resources from the private and public sectors; designing and delivering standard training for the sector; and evaluating training.

In addition, owners, operators, and other IT Sector entities conduct internal training and fund vendor-neutral certifications to ensure that their employees are appropriately trained. Examples of internal training include training related to risk assessments, risk management, cost-benefit analysis, and related concepts.

6.3 Roles and Responsibilities

The following sections outline SSA, SCC, GCC, and shared responsibilities.

6.3.1 Sector-Specific Agency

NCSD has responsibility for working with public and private IT Sector security partners to promote not only the physical, human, and cyber elements of the infrastructure but also the cyber security of all infrastructure sectors as consumers of IT. NCSD responsibilities are as follows:

- **Coordinate development and drive implementation of the IT SSP:**
 - Coordinate efforts to compose and maintain the IT SSP;
 - Support implementation of the collaboratively developed risk assessment approach for the IT Sector;
 - Coordinate efforts to determine protective measures for the IT Sector;
 - Identify R&D requirements and conduct R&D in concert with other government entities, the private sector, and other security partners;
 - Ensure public and private sector security partners are engaged, as early as possible, in the development and revision of the SSP and in planning other CI/KR protection initiatives;
 - Encourage and promote participation in the IT GCC, IT SCC, and IT-ISAC; and
 - Support the IT-ISAC as the operational information-sharing mechanism for the private sector.
- **Engage with IT Sector security partners:**
 - Identify relevant public and private sector security partners that have a role in securing the IT Sector;
 - Develop a plan for regular engagement between NCSD and the public and private IT Sector security partners;

- Promote security awareness within the IT Sector;
- Communicate timely, analytical, and useable information, including threat and warning information, specific to the infrastructure and public and private IT Sector security partners;
- Identify incentives for the private sector to undertake voluntary efforts to improve security (physical, cyber, and human) and implement the SSP;
- Encourage the use of risk transfer mechanisms, such as contractual arrangements that expand the use of state-of-the-art security practices through market mechanisms; and
- Develop a business case for continuing investment in securing the IT Sector.
- **Engage with other government entities:**
 - Work with the intelligence and law enforcement communities to enhance the collection, assessment, and distribution of cyber-related intelligence to IT Sector security partners;
 - Solicit input from government entities on IT Sector CI/KR protection-related efforts;
 - Work with US-CERT to provide cyber alerts, response assistance, and information on remediation measures to public and private sector security partners; and
 - Interact with other SSAs and sectors to identify unique dependencies, interdependencies, relationships, and partnerships across sectors.

6.3.2 IT Sector Coordinating Council³⁶

The IT SCC's responsibilities are as follows:

- **Develop and drive implementation of the IT SSP:**
 - Participate in the development, review, and enhancement of the IT SSP;
 - Support the identification and risk assessment of critical IT Sector functions;
 - Collaborate with NCSA and other public IT Sector security partners to identify current and future protective program needs;
 - Encourage and share advances in security resulting from R&D; and
 - Use the IT-ISAC as the focal point for operational information sharing with the private sector.
- **Engage with IT public sector security partners to promote CI/KR protection:**
 - Identify relevant public sector security partners that have a role in securing the IT Sector; and
 - Promote security awareness within the IT Sector.

6.3.3 IT Government Coordinating Council³⁷

The IT GCC has responsibility for coordination of strategies, activities, policy, and communications across government entities with a role in securing the IT Sector. The IT GCC's responsibilities are as follows:

- **Develop and facilitate implementation of the IT SSP:**
 - Lead efforts to develop, review, enhance, and maintain the IT SSP;

³⁶ For a complete list of IT SCC members, see section 1.4

³⁷ For a complete list of IT GCC members, see section 1.4.

- Support the identification and risk assessment of critical IT Sector functions;
- Collaborate with private IT Sector security partners to identify current and future IT Sector protective program needs; and
- Encourage and share advances in security resulting from R&D.
- **Engage with IT private sector security partners to promote CI/KR protection:**
 - Identify relevant private sector security partners that have a role in the security of the IT Sector;
 - Participate in the sector partnership model to coordinate with IT Sector security partners;
 - Use available communication tools (e.g., HSIN-CS, Web site, and telephone hotline) to exchange information with the private sector in relation to the IT Sector; and
 - Promote security awareness within the IT Sector.

6.3.4 Shared Cross-Sector Cyber Security Responsibilities

Various critical IT Sector functions are consumed by other critical infrastructure sectors and by Federal, State, and local governments. The IT Sector provides the ability to secure IT products and services; however, each sector is individually responsible for the day-to-day operational security of its cyber systems. The IT Sector has an understanding of not only how its products and services are used by consumers, but also an understanding of the security challenges that other sectors face as they use their cyber infrastructure. Public and private IT Sector security partners leverage this expertise to assist other CI/KR sectors and governments in addressing cyber security.

6.4 Actions

The following bulleted list includes near term and long term actions to be completed to implement this section of the SSP.

6.4.1 Near Term (~1 year)

- Update the IT SSP annually. (GCC and SCC)
- Develop (annually) the IT Sector CI/KR Protection Annual Report. (NCSD with GCC and SCC input)
- Identify necessary resources to implement the IT SSP risk management approach, protective programs, information sharing mechanisms, R&D initiatives, and performance measurement. (NCSD, GCC, and SCC)
- Engage with and develop public sector programs to support the implementation and maintenance of the IT SSP. (NCSD)
- Coordinate closely with the Communications Sector on the development of the next Communications SSP. (GCC and SCC)

6.4.2 Long Term (1-3 years)

- Develop and facilitate training and education initiatives necessary to implement the IT SSP successfully. (NCSD, GCC, and SCC)
- Collaborate with the Communications Sector on outreach and education to customers on their reliance on Communications and IT infrastructures and security roles and responsibilities. (NCSD, GCC, SCC, NCS, Communications SCC, and Communications GCC)
- Fulfill the roles and responsibilities identified in section 6.3. (All)

7. Implementing the SSP and Tracking Progress

Tracking the implementation progress of the actions set forth in this plan is essential to the SSP's success. A collaborative process that benefits from the voluntary input of IT SCC and IT GCC representatives can most accurately track the SSP's implementation. Tracking SSP implementation provides public and private sector security partners with a shared understanding of the progress toward achieving the sector's goals. This section describes the IT Sector's demonstration of successful SSP implementation in support of its goals and objectives.

7.1 Tracking Progress Challenges

The IT SSP contains clear goals and objectives supported by specific action items. Implementing those action items in support of sector goals and objectives is a responsibility shared by public and private sector security partners. Implementing and tracking the action items requires commitment and resources (e.g., financial, time, personnel, and specific expertise) from the public and private sectors. Dedicated financial and personnel resources also may be required to implement and accurately track the progress of the SSP. Public and private sector security partners will need to prioritize the actions in this plan and proceed with implementation and tracking using an iterative approach that takes resource availability into account.

7.2 Measurement Overview

The IT Sector has a diverse operating environment that is marked by continuous evolution, convergence, and heterogeneous architectures, networks, technologies, and businesses. With such diversity across the IT infrastructure, security partner base, and key functions, traditional quantitative measurement approaches are not ideally suited to the IT Sector. For example, a quantitative measure to assess the risk mitigation efforts of ISPs would have little utility for assessing the risk mitigation efforts of IT system integrators. Therefore, the IT Sector's approach will rely on qualitative, implementation-focused measurement. The IT Sector focuses on identifying and tracking public and private sector progress in implementing SSP action items. The IT Sector's approach will track the sector's progress toward achieving its goals with respect to four key categories:

- **One-time activities described in the IT SSP.** These are one-time SSP action items (e.g., implementing a specific protective program).
- **Recurring activities described in the IT SSP.** These are recurring SSP activities (e.g., reports and conferences).
- **Private sector self-directed activities.** These are activities undertaken by the IT industry that are outside the scope of the SSP, but still contribute to the overall IT Sector goals (e.g., security standards development).

- **Public sector self-directed activities.** These are activities undertaken by Federal, State, and local governments that are outside the scope of the SSP but still contribute to the overall IT Sector goals.

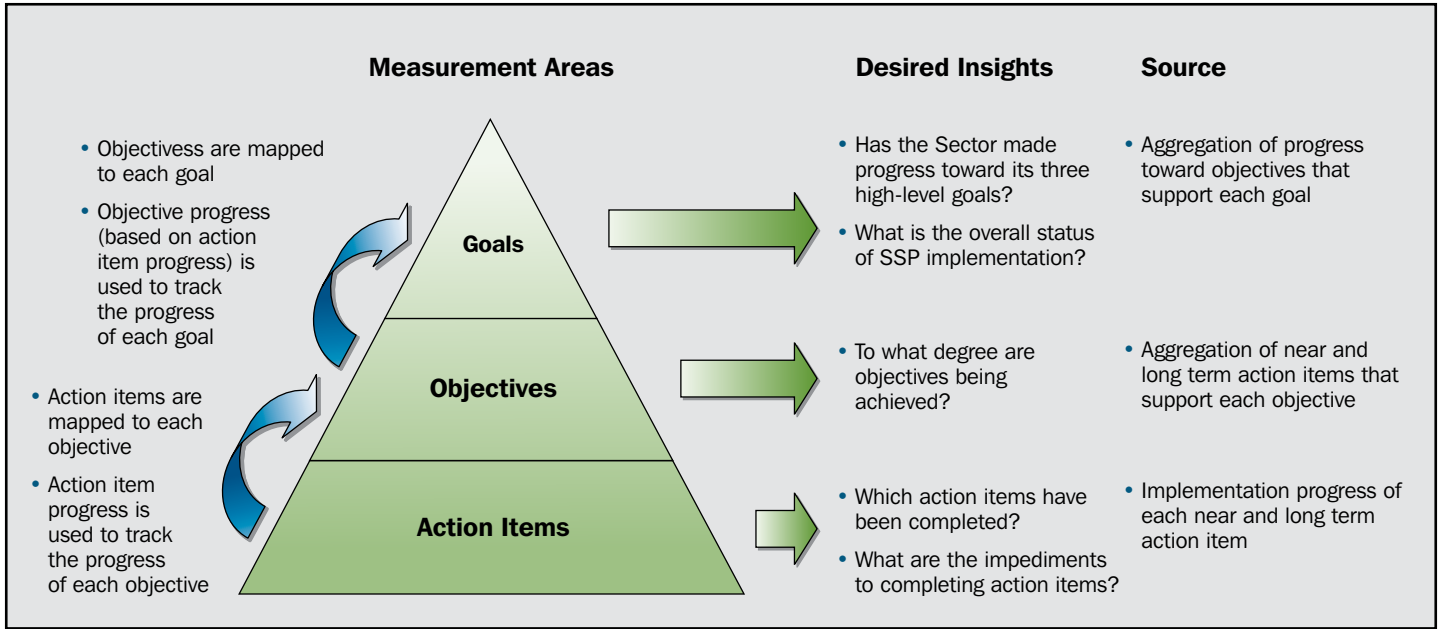
All suggested SSP action items support the sector’s goals. Therefore, implementation of action items serves as an indicator of progress toward a sector goal.

7.3 Measurement Approach

The IT Sector’s approach will track progress against sector goals iteratively. As figure 7.1 illustrates, the near- and long-term action items described in each section and the public and private sector self-directed activities will serve as the foundation of the sector’s measurement approach.

As also shown in figure 7-1, the measurement approach is hierarchical—each action is mapped to a specific sector objective, which is mapped to a sector goal. Therefore, each objective is met when the action items that support it are implemented. Thus, an evaluation of the implementation of the action items yields insights into the support of each objective. Similarly, the implementation of each objective yield insight into the progress the sector has made toward each goal. By using this approach, NCS&D, the IT SCC, and IT GCC can gain insights into implementation progress and provide actionable outputs that can guide sector activities to ensure that goals are being supported.

Figure 7-1: IT Sector Measurement Approach

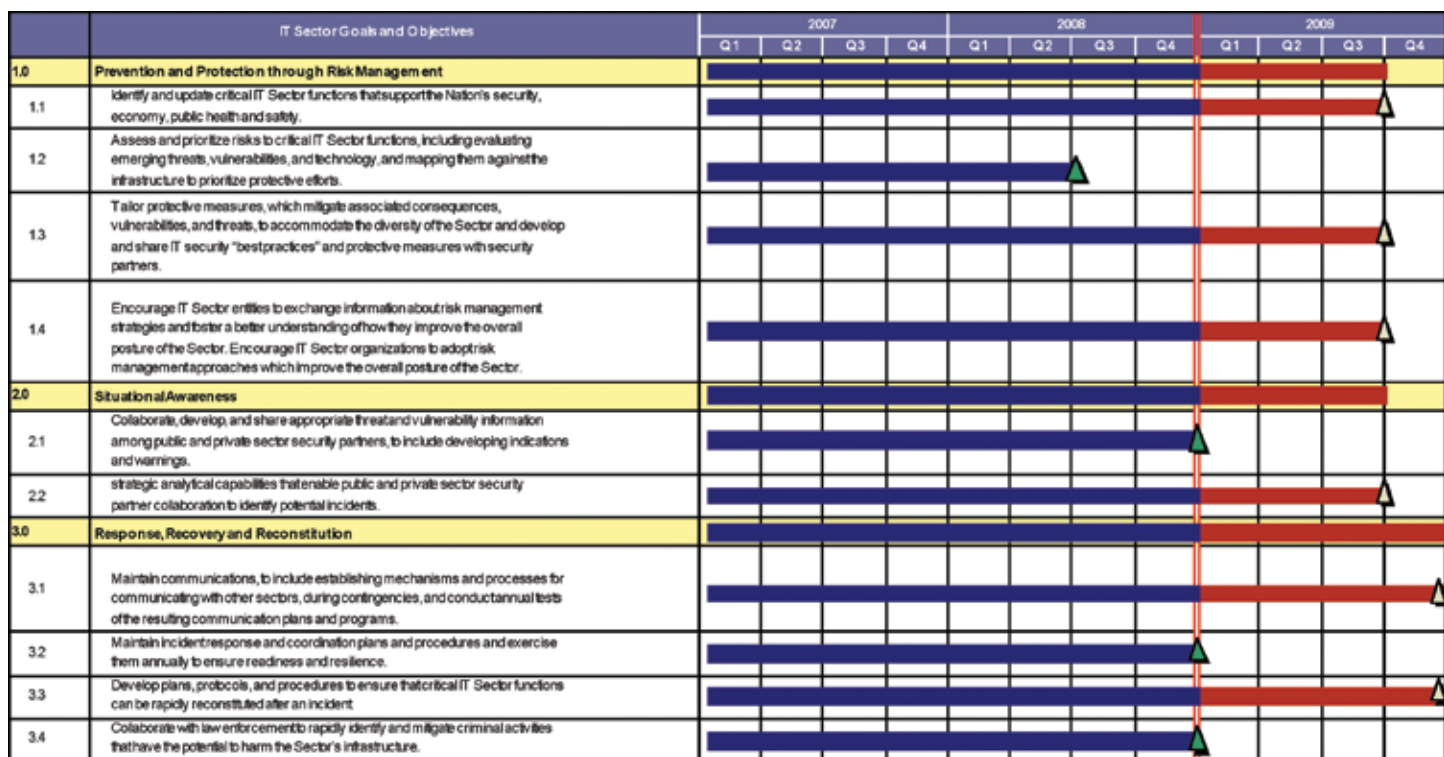


7.4 Goals and Objectives Measurement

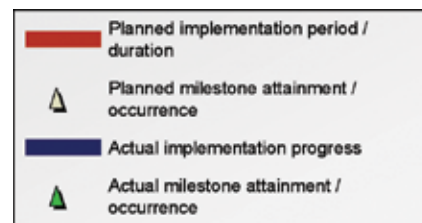
To illustrate implementation levels and goal support, the IT SCC and IT GCC will rely on Gantt charts to show activity, duration, and completion. A Gantt chart is a modified bar chart that shows duration and milestones of key activities within a project framework.

Figure 7-2 is a notional Gantt chart to track IT SSP implementation at the highest level of the measurement hierarchy—goals and objectives. Figure 7-2 illustrates how IT Sector progress could be reported in future iterations of the SSP or for IT Sector CI/KR Protection Annual Report purposes—in this example, at the end of the fourth quarter (Q4) of 2008. Objective 1.1 provides a hypothetical example of how activities that support objective 1.1 may have been implemented from Q1 2007 through Q4 2008. The planned duration of implementation is through Q3 2009, as indicated by the beige triangle. Objective 1.2 illustrates that all activities were implemented from Q1 2007 through Q2 2008, which concluded all required actions for objective 1.2 as indicated by the green triangle. The overall performance of goal 1 implementation is measured in row 1.1 and is a product of the implementation of the activities supporting the objectives that support goal 1.

Figure 7-2: Notional Gantt Chart to Indicate Goal and Objective Implementation Progress at Q4 2008



By observing the planned and actual implementation periods and milestones, the IT SCC and IT GCC can determine the implementation progress of SSP action items. The level of implementation then can be used to determine the extent to which the sector is achieving its goals.



7.5 Activities Implementation

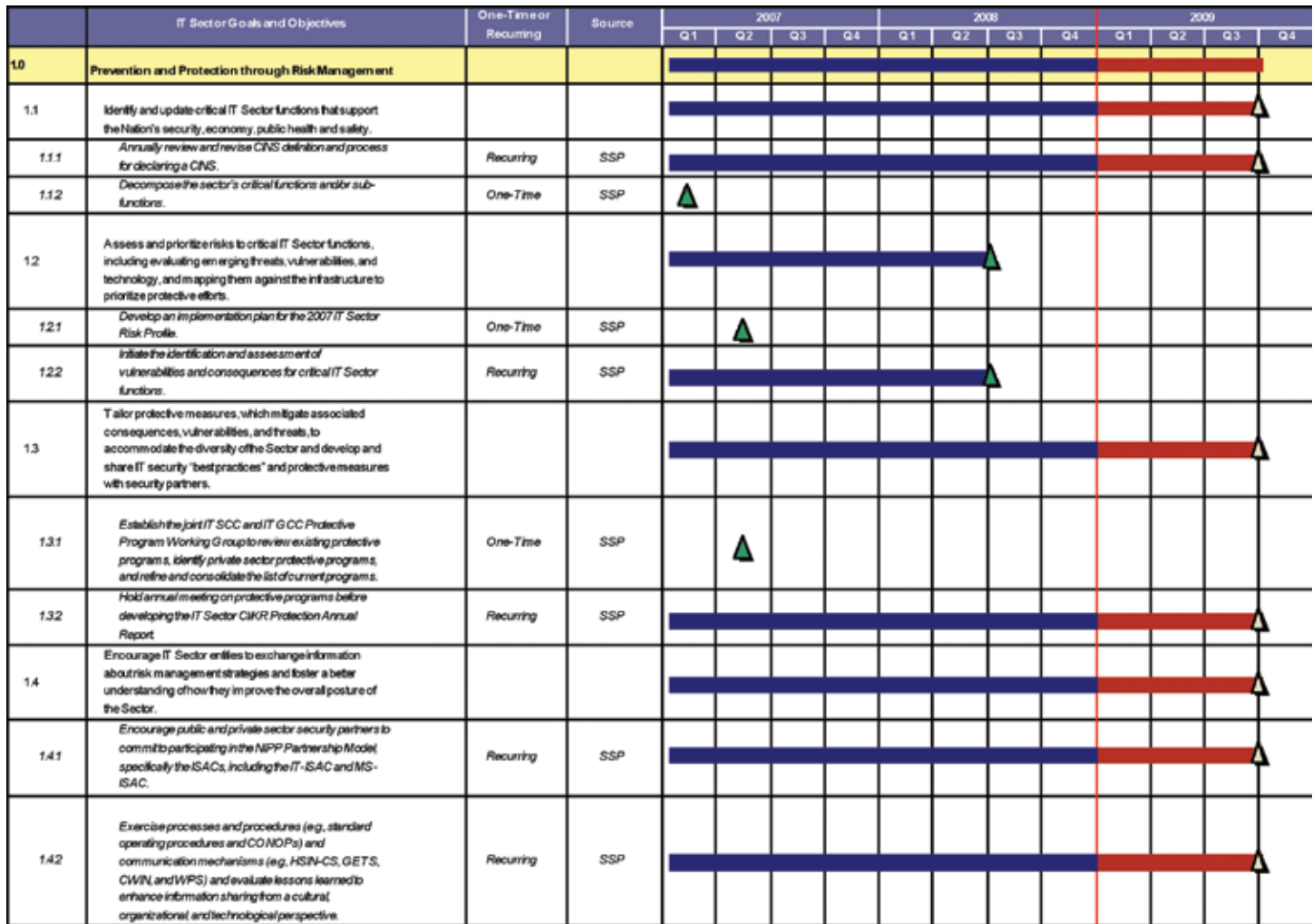
The goals and objectives implementation measures are an aggregation of the implementation of near-and long-term activities from across four categories:

- One-time activities described in the IT SSP;
- Recurring activities described in the IT SSP;
- Private sector self-directed activities; and
- Public sector self-directed activities.

Together, NCSD, the IT SCC, and IT GCC will develop Gantt charts that illustrate the implementation progress of sector activity across the four categories outlined above, each mapped to a specific objective and goal. Figure 7-2 displays a notional Gantt chart that illustrates the type of detail that will be offered. Note that figure 7-3 provides more granular details about the information presented in figure 7-2 by illustrating the implementation levels of each activity that support the Objectives.

For example, figure 7-3 shows that activity 1.1.1 is a *recurring activity* identified in the SSP that has been continually implemented from Q1 2007 through Q4 2008 and has a planned conclusion date of Q3 2009. In addition, activity 1.1.2 was a *one-time activity* that was completed in Q1 2007. Thus, overall, Objective 1.1 has been continually implemented since Q1 2007 and is planned to conclude in Q3 2009. Similarly, all activities that support the objectives under goal 1 are on schedule as of Q4 2008 and all are planned to be completed by Q3 2009. Figure 7-3 shows the progression from *action item* to *objective* to *goal* and provides a granular view of how the sector is implementing actions to support its goals. Once the measurement approach is implemented, subsequent SSP iterations will contain progress updates and associated next steps based on the sector's progress tracking activities.

Figure 7-3: Notional Gantt Chart to Indicate Activity Implementation Progress at Q4 2008



7.6 Reporting on Progress

Tracking the implementation progress of actions within this SSP will require the commitment and resources of the IT SCC and IT GCC. The IT SCC and IT GCC will use the following approach for accurate tracking of the implementation progress of action items contained within the SSP:

- As noted in this SSP, each action item has an entity/organization who will be the party responsible for its implementation (e.g., IT-ISAC, NCSD, GCC, and SCC).
- Responsible parties will monitor progress of their action items within the SCC or GCC.
 - For each private sector (IT SCC) action item:
 - The IT SCC (as the lead policy arm) will examine each SSP action item that falls under its purview and will decompose it into measurable components to assess its implementation progress; and

- The IT SCC will collect progress information about each SCC action item from members at IT SCC meetings and aggregate the information to the level of the notional Gantt chart in figure 7-3.
- For each public sector (IT GCC) action item:
 - As appropriate, the IT GCC will examine each action item that falls under its purview and decompose it into measurable components to assess its implementation progress; and
 - NCSD will collect progress information on each IT GCC-related action item from members at IT GCC meetings and aggregate the information to the level of the notional Gantt chart in figure 7-3.
- For action items that require joint public and private sector collaboration:
 - The IT SCC and IT GCC will examine each such action item and decompose it into measurable components to assess its implementation progress; and
 - The IT SCC and IT GCC will collect progress information on each such action item from their constituencies at IT SCC and IT GCC meetings and collectively aggregate the information to the level of the notional Gantt chart in figure 7-3.
- The IT SCC and IT GCC will combine their progress data to track overall SSP progress for reporting purposes (i.e., IT Sector CI/KR Protection Annual Report) and for subsequent SSP iterations.

7.7 Actions

The following bulleted list includes near and long term actions to be completed to implement this section of the SSP.

7.7.1 Near Term (~1 year)

- Prioritize sector action items, taking into consideration available resources. (NCSD, SCC, GCC)
- Create Gantt chart for the sector that maps SSP actions to objectives and goals. (NCSD with input from SCC and GCC)

7.7.2 Long Term (1-3 years)

- Continue to reassess action item prioritization based on evolving status of the sector and resource availability. (NCSD, SCC, and GCC)
- Track sector action item progress and update the IT SSP. (NCSD, SCC, and GCC)

Appendix 1: List of Acronyms and Abbreviations

APWG	Anti-Phishing Working Group	COTS	Commercial Off-the-Shelf
AT-SPI	Anti-Tamper–Software Protection Initiative	CVE	Common Vulnerabilities and Exposures
BGP	Border Gateway Protocol	CWIN	Critical Infrastructure Warning Information Network
CAEIAE	National Centers of Academic Excellence in Information Assurance Education	DC3	Defense Cyber Crime Center
CALEA	Communications Assistance for Law Enforcement Act	DOD	Department of Defense
CARC	Community Acquisition Risk Center	DCFL	DOD Computer Forensics Laboratory
CCIPS	Computer Crimes and Intellectual Property Section	DCCI	DOD Cyber Crime Institute
CCEVS	Common Criteria Evaluation and Validation Scheme	DCITP	DOD Computer Investigations Training Program
CFIUS	Committee on Foreign Investment in the United States	DHS	Department of Homeland Security
CI	Counterintelligence	DNI	Director of National Intelligence
CIDDAC	Cyber Incident Detection Data Analysis Center	DNS	Domain Name System
CII Act	Critical Infrastructure Information Act of 2002	DOJ	Department of Justice
CI/KR	Critical Infrastructure and Key Resources	DPA	Defense Production Act
CIO	Chief Information Officer	DRII	Disaster Recovery Institute International
CIP	Critical Infrastructure Protection	ECPA	Electronic Communications Privacy Act
CIPAC	Critical Infrastructure Partnership Advisory Council	ECTF	Electronic Crimes Task Forces
COBIT	Control Objectives for Information and Related Technology	EO	Executive Order
COD	Common Operating Database	ESF	Emergency Support Function
ConOps	Concept of Operations	FBI	Federal Bureau of Investigation
COP	Common Operating Picture	FCPA	Foreign Corrupt Practices Act
		FISMA	Federal Information Security Management Act
		FOIA	Freedom of Information Act
		FOUO	For Official Use Only

NTOC	National Security Agency Threat Operations Center
NVD	National Vulnerability Database
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation
OECD	Organisation for Economic Co-operation and Development
OGC	Office of Government Commerce (United Kingdom)
OIP	Office of Infrastructure Protection
OMB	Office of Management and Budget
OSTP	Office of Science and Technology Policy
OVAL	Open Vulnerability Assessment Language
PC	Personal Computer
PCII	Protected Critical Infrastructure Information
PCIS	Partnership for Critical Infrastructure Security
PDD	Presidential Decision Directive
PITAC	President's Information Technology Advisory Committee
POC	Point of Contact
PSN	Public Switched Network
PSTN	Public Switched Telephone Network
R&D	Research and Development
RFI	Request for Information
RISS	Regional Information Sharing System
RMD	Risk Management Division
ROI	Return on Investment
S&T	Science and Technology
SBU	Sensitive But Unclassified
SCC	Sector Coordinating Council
SFS	Federal Cyber Service: Scholarship For Service
SHIRA	Strategic Homeland Infrastructure Risk Assessment
SIP	Session Initiation Protocol
SLFC	State and Local Fusion Center
SLGCP	State and Local Government Coordination and Preparedness

SME	Subject Matter Expert
SOX	Sarbanes-Oxley Act
SSA	Sector-Specific Agency
SSE-CMM®	Systems Security Engineering-Capability Maturity Model
SSP	Sector Specific Plan
TLD	Top Level Domain
TOPOFF	Top Officials
TSP	Telecommunications Service Priority
U.S.	United States
US-CERT	United States Computer Emergency Readiness Team
USSS	United States Secret Service
VoIP	Voice over Internet Protocol
WebEOC	Web Emergency Operations Center
WMD	Weapon of Mass Destruction
WPS	Wireless Priority Service



Appendix 2: Authorities

Key authorities for the IT Sector address the establishment of the IT Sector, its availability, resilience, and security, and provide guidance on sector coordination and specific programs. This appendix provides a brief description of major authorities with relevance to IT Sector CIP activities.

Homeland Security/National Security IT Authorities

- **The Homeland Security Act of 2002** (November 2002). The Homeland Security Act established the following specific CI/KR protection roles and responsibilities for the DHS:
 - Developing a comprehensive national plan for securing the CI/KR of the United States;
 - Providing crisis management in response to attacks on critical information systems;
 - Providing technical assistance to the private sector and other government entities with respect to emergency recovery plans for failures of critical information systems; and
 - Coordinating with other agencies of the Federal Government to provide specific warning information and advice about appropriate protective measures and countermeasures to State, local, and nongovernmental organizations.
- **HSPD-7, Critical Infrastructure Identification, Prioritization, and Protection** (December 2003). HSPD-7 establishes a national policy for Federal departments and agencies to identify and prioritize U.S. CI/KR and to protect them from attack. HSPD-7 identified Telecommunications and IT as distinct sectors and assigned oversight for both to the DHS: NCS serves as the lead DHS agency for the Telecommunications Sector, and NCSD serves as the lead agency for the IT Sector. Specifically, HSPD-7 charges the DHS with maintaining an organization—NCSD—to serve as a focal point for the security of cyberspace and facilitate interactions and collaborations between and among Federal departments and agencies, State and local governments, the private sector, academia, and international organizations. The NCSD mission includes analysis, warning, information sharing, vulnerability reduction, mitigation, and aiding national recovery efforts for critical infrastructure information systems. NCSD supports the Department of Justice (DOJ) and other law enforcement agencies in their continuing missions to investigate and prosecute threats to and attacks against cyberspace, to the extent permitted by law. To the extent permitted by law, Federal departments and agencies with cyber expertise, including the Departments of Justice, Commerce, Treasury, Defense, Energy, and State, and the Central Intelligence Agency, will collaborate with and support NCSD in accomplishing its mission.
- **Intelligence Reform and Terrorism Prevention Act of 2004** (December 2004). This act represents the most dramatic reform to the Nation's intelligence capabilities since the National Security Act of 1947. This authority requires the President

to establish an information-sharing environment (ISE) to facilitate the sharing of terrorism information among all appropriate Federal, State, regional, local, and tribal government and private sector entities, through the use of policy guidelines and technologies; to include provisions for privacy and civil liberty rights; to establish programs for the enhancement of public safety communications interoperability; and to recommend that the DHS promote the adoption of voluntary national preparedness standards for the private sector. The act and subsequent authorization legislation established the position of the Director of National Intelligence (DNI) and give the DNI and DNI/Chief Information Officer (CIO) significant additional authorities and responsibilities regarding the management of the IC and its role in critical infrastructure protection.

- **Presidential Memorandum for the Heads of Executive Departments and Agencies: Guidelines and Requirements in Support of the Information-Sharing Environment** (December 2005). This Presidential memorandum outlines information-sharing authorities and directs executive departments and agencies, in consultation with the program manager for information sharing, to leverage ongoing information-sharing efforts in development of the ISE and to promote a culture of information sharing. In addition, this memorandum provides the following guidelines for the ISE: define common standards for how information is acquired, accessed, shared, and used within the ISE; develop a common framework for the sharing of information between and among executive departments and agencies and State, local, and tribal governments, law enforcement agencies, and the private sector; standardize procedures for SBU information; facilitate information sharing between executive departments and agencies and foreign partners; and protect the information privacy rights and other legal rights of Americans.
- **Executive Order (EO) 13311 (as amended by EO 13388), Homeland Security Information Sharing** (October 2005). This EO creates an ISE to facilitate the sharing of terrorism information and restructures the Information Sharing Council.
- **Executive Order 13353, Establishing the President's Board on Safeguarding American's Civil Liberties** (August 2004). This EO further strengthens protections for the rights of Americans, including freedoms, civil liberties, and information privacy guaranteed by Federal law, in the effective performance of national security and homeland security functions. Accordingly, this EO establishes the President's Board on Safeguarding Americans' Civil Liberties, chaired by DOJ, which advises the President on information-sharing policy issues.
- **HSPD-5, Management of Domestic Incidents** (February 2003). This directive enhances the United States' ability to manage domestic incidents by establishing a single, comprehensive NRP. HSPD-5 places initial responsibility for domestic incident management on State and local authorities but states that the Federal Government will become involved when State and local resources are overwhelmed or Federal interests are involved. This directive also recognizes the role played by private and nongovernmental sectors in preventing, preparing for, responding to, and recovering from terrorist attacks, major disasters, and other emergencies, and orders the Secretary of Homeland Security to coordinate with private and nongovernmental sectors to ensure adequate planning, equipment, training, and exercise activities, and to promote partnerships to address incident management capabilities.
- **HSPD-8, National Preparedness** (December 2003). This directive establishes policies to strengthen the preparedness of the United States to prevent and respond to threatened or actual domestic terrorist attacks, major disasters, and other emergencies by requiring a national domestic all-hazards preparedness goal, establishing mechanisms for improved delivery of Federal preparedness assistance to State and local governments, and outlining actions to strengthen preparedness capabilities of Federal, State, regional, local, and tribal entities.
- **HSPD-9, Bio Defense Strategy** (April 2004). This directive establishes national policy that prioritizes the protection of critical infrastructure (physical and cyber) from the effects of biological weapons attacks. A biological weapons attack might deny access to essential facilities and response capabilities. Therefore, it is necessary to improve the survivability and ensure the continuity and restoration of operations of critical infrastructure sectors following biological weapons attacks. Assessing the vulnerability of this infrastructure—particularly, the medical, public health, food and agriculture, water, energy, and transportation sectors—is the focus of current efforts. The DHS, in coordination with other appropriate Federal departments and

agencies, leads these efforts, which include developing and deploying biodetection technologies and decontamination methodologies. This HSPD is relevant because human elements of critical IT Sector functions exist. If this human element were affected by a biological attack, cascading effects might occur. For example, if an antivirus vendor organization's campus were affected, the skills and knowledge needed to perform virus definition updates and patching potentially might be unavailable during a crucial time.

- **HSPD-12, Policy for a Common Identification Standard for Federal Employees and Contractors** (August 2004). This directive establishes national policy to enhance security, increase government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees). Secure and reliable forms of identification for purposes of this directive means identification that: (1) is issued based on sound criteria for verifying an individual employee's identity; (2) is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation; (3) can be rapidly authenticated electronically; and (4) is issued only by providers whose reliability has been established by an official accreditation process. IT Sector technologies and infrastructure facilitate the implementation of this directive, and future developments in the sector can affect efforts to maintain the common identification standard.
- **Executive Order (EO) 13231 (as amended by EO 13286 as of February 2003), Critical Infrastructure Protection in the Information Age** (October 2001). This EO ensures the protection of information systems for critical infrastructure, including emergency preparedness communications, and the physical assets that support such systems in the information age.
- **Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001** (October 2001). This act affects companies' IT departments because they must be prepared to provide terrorism-related information to the FBI if subpoenaed.
- **Export Administration Act of 1979, as amended (EAA)**, implemented through the Export Administration Regulations (August 2006). The EAA authorizes the Secretary of Commerce to regulate exports of commodities, software, and technology (collectively referred to as "items") based on national security and foreign policy objectives. Under the EAA, controls are placed on exports of items based on the technical capabilities of such items and also based on the destination of such exports. The EAA currently is lapsed, but the Export Administration Regulations remain in effect through the International Emergency Economic Powers Act (described below), Executive Order 13222, and the Presidential Notice of August 3, 2006.
- **Exon-Florio Amendment to the Defense Production Act and Executive Orders 11858, 12188, and 12661** (May 1975, January 1980, and December 1988). These provisions authorized the creation of the Committee on Foreign Investment in the United States (CFIUS), which is an interagency committee chaired by the Department of the Treasury. The mission of CFIUS is to review and potentially recommend that the President block foreign acquisitions of U.S. companies that threaten to impair national security.
- **International Emergency Economic Powers Act (IEEPA)** (October 1977). This act authorizes the President to engage in a wide variety of activities to deal with an unusual and extraordinary threat to the country's national security, foreign policy, or economy. To trigger authorities under IEEPA, the threat must originate in whole or substantial part from outside the United States, and the President must declare a national emergency with respect to such threat. Using IEEPA, the President has continued the Export Administration Regulation in effect despite the lapse of the EAA, as amended (see above).

National Strategies

- **The National Strategy for Homeland Security** (July 2002). The National Strategy for Homeland Security characterizes terrorism as any premeditated, unlawful act dangerous to human life or public welfare intended to intimidate or coerce civilian populations or governments. This description captures the core concepts shared by the various definitions of terrorism contained in the U.S. Code, each crafted to achieve a legal standard of specificity and clarity. This description covers kidnappings;

hijackings; shootings; conventional bombings; attacks involving chemical, biological, radiological, or nuclear weapons; cyber attacks; and any number of other forms of malicious violence. Terrorists can be U.S. citizens or foreigners, acting in concert with others, on their own, or on behalf of a hostile nation. Terrorists may seek to cause widespread disruption and damage, including casualties, by attacking our electronic and computer networks, which are linked to other critical infrastructures such as our energy, financial, and securities networks. Terrorist groups already are exploiting new information technology and the Internet to plan attacks, raise funds, spread propaganda, collect information, and communicate securely. As terrorists further develop their technical capabilities and become more familiar with potential targets, cyber attacks will become an increasingly significant threat. Accordingly, DHS will place an especially high priority on protecting our cyber infrastructure. Actions to reduce America's vulnerability to terrorism also must harness the coordinated effort of many Federal departments and agencies that have highly specialized expertise and long-standing relationships with industry.

- **The National Strategy to Secure Cyberspace** (July 2002). This strategy states that a top priority for the Nation is to understand infrastructure interdependencies and improve the physical security of cyber systems and telecommunications. The strategy directs DHS to work with State and local governments to establish strong IT security programs. It also describes the National Cyberspace Security Response System.
- **National Strategy for the Physical Protection of Critical Infrastructures and Key Assets** (February 2003). This national strategy puts forth strategic objectives to identify and assure the physical protection of critical infrastructure and assets; to provide timely warning and assure the protection of those infrastructures and assets that face a specific, imminent threat; and to assure the protection of infrastructures and assets that may become targets over time by pursuing specific initiatives and enabling a collaborative environment between the public and private sector.
- **National Counterintelligence Strategy** (March 2005). This strategy seeks to ensure that industry is not disadvantaged by foreign intelligence operations and provides appropriate threat information to industry and IT security partners to take appropriate risk mitigation measures. The strategy recognizes that the U.S. strategic response to today's threats require that the Nation's counterintelligence capabilities need to address technical, cyber, and human threats.

Management and Acquisition of Federal Government Information Technology

- **Clinger-Cohen Act of 1996** (AKA Information Technology Management Reform Act) (February 1996). Recognizing the importance of IT for effective government, Congress and the President enacted the Information Technology Management Reform Act and the Federal Acquisition Reform Act. These two acts, together known as the Clinger-Cohen Act, require the heads of Federal agencies to link IT investments to agency accomplishments. The Clinger-Cohen Act also requires that agency heads establish a process to select, manage, and control their IT investments. This act also reformed the way the Federal Government acquires and manages IT through performance-based and results-based management. The law focuses on IT investment management, information resources management, and IT management. It also directs all Federal agencies to use a formal enterprise architecture process. It transferred IT responsibilities from the General Services Administration (GSA) to OMB and further defined the role of an agency's CIO.
- **Executive Order (EO) 13011, Federal Information Technology** (January 2003). This EO outlines a coordinated IT approach that builds on current structures and successful practices to improve Federal Government mission performance and service delivery. Establishes the CIO Council, Government Information Technology Services Board, and Information Technology Resources Board to advise the President in carrying out the responsibilities of the Clinger-Cohen Act.
- **Memorandum to Heads of Selected Departments and Agencies, Interagency Support for Information Technology** (March 1997). This memorandum institutes funds for carrying out EO 13011.

- **Federal Acquisition Regulation, Part 39, Acquisition of Information Technology** (February 2006). This regulation establishes acquisition policies and procedures for acquiring information and IT (excluding national security systems).
- **E-Government Act of 2002** (January 2002). This act improves electronic Federal Government processes and services promotion and management through the establishment of a Federal CIO at OMB. The act establishes a measurement framework that requires using Internet-based IT to help citizens gain better access to services and information.
- **The Paperwork Reduction Act of 1995** (May 1995). This act establishes that the OMB Director will develop and oversee the “implementation of policies, principles, standards, and guidelines for information technology functions and activities of the Federal Government” to help enhance agency mission performance.
- **Federal Information Security Management Act (FISMA)** of 2002 (November 2002). This act establishes a framework for the security of the Federal Government’s IT by mandating annual audits of Federal Government entities and those organizations affiliated with the Federal Government.

Information Technology Audit-Related Authorities

- **Health Insurance Portability and Accountability Act (HIPAA)** (August 1996). Seeks to enhance health insurance coverage portability and continuity; stop health insurance and health care delivery waste, fraud, and abuse; foster medical savings accounts; increase long-term care services and coverage access; and make health insurance administration less complicated. The HIPAA Security Rule establishes minimum standards that safeguard electronic protected health information.
- **Gramm-Leach-Bliley Act (GLBA)** (September 1999). This act establishes the way in which personal information about individuals who obtain financial products or services from financial institutions is shared. Three rules manage personally identifiable information: (1) a financial institution is required to provide a customer with a privacy notice; (2) every financial institution is to create an information security plan; and (3) financial institutions must take precautions to prevent pretexting (i.e., obtaining personally identifiable information without proper authority).
- **Sarbanes-Oxley Act (SOX) of 2002** (July 2002). This act establishes policies related to corporate governance, the practice of public accounting, and financial disclosure. Section 404 largely affects every company’s IT department as it outlines processes for addressing such things as installation of new business applications, application monitoring, and IT system and network security.
- **Foreign Corrupt Practices Act (FCPA) of 1977** (15 United States Code (U.S.C.) 78dd-1, et seq.) (November 1988). The FCPA seeks to thwart corporate bribery of foreign officials by requiring companies to maintain accurate books, records, and accounts and by requiring publicly traded companies to retain internal accounting control systems.
- **The Cyber Security Enhancement Act of 2002** (February 2002). The Cyber Security Enhancement Act of 2002 amends Federal computer crime sentencing guidelines, making it possible to issue more appropriate sentences for crimes involving fraud in connection with computers and access to protected information, protected computers, restricted data in interstate or foreign commerce, or involving a computer used by or for the Federal Government.
- **The Computer Fraud and Abuse Act of 1984 as amended by the Computer Abuse Amendments Act of 1994** (September 1994). Note: Section 1030 was amended on October 26, 2001, by the USA PATRIOT antiterrorism legislation. Section 1030: Fraud and related activity in connection with computers states that whoever, having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the U.S. Government pursuant to an executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y of Section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the

United States, or to the advantage of any foreign nation, willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it.

National Preparedness and Response Authorities Related to Information Technology

- **Executive Order (EO) 12656, Assignment of Emergency Preparedness Responsibilities** (November 1988). This EO delegates national security and emergency preparedness (NS/EP) responsibilities to Federal departments and agencies and instructs agencies to create plans and capabilities that will ensure continuity of essential operations.
- **Defense Production Act of 1950, as amended (DPA)** (June 1998). This act authorizes the President to, among other things, demand that companies accept and give priority to Federal Government contracts that the President “deems necessary or appropriate to promote the national defense.” In 2003, the DPA was amended, so that the term “national defense” includes “critical infrastructure protection and restoration.” The act authorizes the provision of financial incentives for certain technological development and domestic production.
- **National Response Plan** (December 2004). Emergency Support Function (ESF) #2, Communications, coordinates Federal actions to support temporary NS/EP telecommunications and telecommunications infrastructure restoration. During response efforts, ESF#2 supports all Federal departments and agencies in the procurement and coordination of all NS/EP telecommunications services from the telecommunications and IT industry. The Cyber Security Incident Annex outlines policies, responsibilities, organization, and actions so that the Nation can prepare for, respond to, and recover from nationally significant events related to cyber.
- **The Robert T. Stafford Disaster Relief and Emergency Assistance (Stafford) Act** (October 2000). The Stafford Act gives the President authority to declare a major disaster so Federal resources can be mobilized and distributed to provide relief to the affected States. Assistance is authorized for preparedness, emergency response, and recovery efforts, which involve the IT sector.

Information Technology Communications Related Authorities

- **Communications Act of 1934** (June 1934). This act regulates interstate and foreign wire or radio communication and established the Federal Communications Commission.
- **Telecommunications Act of 1996** (January 1996). Title V of the Telecommunications Act, entitled The Communications Decency Act of 1996, criminalizes the intentional electronic transmission of any communications that is obscene or indecent and prohibits the use of a computer network for the purpose of annoying or harassing recipients of messages.
- **Communications Assistance for Law Enforcement Act (CALEA)** (October 1994). CALEA, as it relates to IT, further defines the existing statutory obligation of telecommunications carriers to assist law enforcement in executing electronic surveillance of communications, such as VoIP and electronic messaging, pursuant to court order or other lawful authorization. The objective of CALEA implementation is to preserve law enforcement’s ability to conduct lawfully authorized electronic surveillance while preserving public safety, the public’s right to privacy, and the telecommunications industry’s competitiveness.

Information Technology Privacy Authorities and Information Protection Related Authorities

- **Electronic Communications Privacy Act (ECPA)** (October 1986). This act establishes policies for access, interception, use, disclosure, and privacy protection of electronic communications for wire and electronic communications. ECPA prevents the Federal Government from mandating electronic communications disclosure without appropriate procedure.

- **The National Infrastructure Protection Act** (October 1996). This act defines “protected information” as “information that has been determined by the U.S. Government pursuant to an EO or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph (y) of Section 11 of the Atomic Energy Act of 1954.” The National Infrastructure Protection Act changes the original language of 18 U.S.C. 1030, redefining computer crime from simply stealing information from a Federal computer system to include willfully harming the integrity and availability of the information or information system. The legislation acknowledges the fact that harm can come to information or information systems, not only through disclosure but also in the loss of the availability or integrity of the information that a system contains.

International Standards and Guidelines

- **International Organization for Standardization (ISO) 17799** (June 2005). ISO 17799 is a worldwide technical standard prepared by the British Standards Institution that is widely accepted as one of the definitive standards for information security. It is intended to serve as a single reference point for identifying a range of controls needed for situations where information systems are used in industry and commerce.
- **Organisation for Economic Co-operation and Development (OECD) Guidelines for the Security of Information Systems.** OECD guidelines are intended to raise awareness of risks to information systems and of the safeguards available to meet those risks. Their purpose is to create a general framework to assist individuals in the public and private sectors responsible for the development and implementation of coherent measures, practices, and procedures for the security of information systems; to promote cooperation between the public and private sectors in the development and implementation of such measures, practices, and procedures; to foster confidence in information systems and the manner in which they are provided and used; to facilitate development and use of information systems, nationally and internationally; and to promote international cooperation in achieving security of information systems.



Appendix 3: Common Risk Management Frameworks

Framework	Description
COBIT 3.0/4.0	The IT Governance Institute's (ITGI) COBIT provides a framework for supporting IT governance to assist organizations in ensuring that IT is aligned with the mission of the business, IT enables the business and maximizes benefits, IT resources are used responsibly, and IT risks are managed appropriately (ITGI, 2005).
Disaster Recovery Institute International (DRII)	Provides courses and training on disaster recovery, including activities and programs designed to return an entity to an acceptable condition and the ability to respond to an interruption in services by implementing a disaster recovery plan to restore an organization's critical business functions. (DRII 2004).
ISO 27001	An information security standard published in 2005 by the International Organization for Standardization/ International Electrotechnical Commission (ISO/IEC) entitled Information Technology—Security Techniques—Information Security Management Systems—Requirements. This standard provides requirements for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving a documented Information Security Management System (ISMS).
ISO/IEC 13335	The ISO/IEC guidance on the management of Information and Communication Technology (ICT) security. Part 1 of ISO/IEC 13335 presents the concepts and models fundamental to a basic understanding of ICT security and addresses the general management issues that are essential to the successful planning, implementation, and operation of ICT security. The other parts provide operational guidance on ICT security. Together, these parts can be used to help identify and manage all aspects of ICT security.
ISO/IEC 17799	An information security standard published in 2005 by the ISO/IEC entitled Information Technology—Security Techniques—Code of Practice for Information Security Management. This standard provides best practice recommendations on information security management for use by those who are responsible for initiating, implementing, or maintaining information security management systems.
ISO/IEC 21827	The SSE-CMM®, a process reference model, is focused on the requirements for implementing security in a system or series of related systems that are the ITS domain. Within the ITS domain, the SSE-CMM model is focused on the processes used to achieve ITS—specifically on the maturity of those processes. There is no intent within the SSE-CMM model to dictate a specific process to be used by an organization, let alone a specific methodology.
ITIL Security Management	The United Kingdom's Office of Government Commerce (OGC) ITIL Security Management provides a framework for assisting organizations in ensuring that security controls are implemented and maintained to address changing circumstances, such as changed business and IT service requirements, IT architecture elements, and threat; that security incidents are managed; that audit results show the adequacy of security controls and measures taken; and that reports are produced to show the status of information security (OGC 2005).

Framework	Description
NIST Special Publication 800-12	The <i>NIST Handbook</i> provides a broad overview of computer security to help readers understand their computer security needs and develop a sound approach to the selection of appropriate security controls. It provides assistance in securing computer-based resources (e.g., hardware, software, and information) by explaining important concepts, cost considerations, and interrelationships of security controls. (NIST 2004).
NIST Special Publication 800-30	The <i>NIST Risk Management Guide for Information Technology Systems</i> provides a framework for developing effective risk management programs within organizations. This guide defines risk management as the process of identifying risk, assessing risk, and taking steps to reducing risk to an acceptable level (NIST 2002).
NIST Special Publication 800-53	The <i>NIST Recommended Security Controls for Federal Information Systems</i> provides guidelines for selecting and specifying security controls for information systems supporting the executive agencies of the Federal Government. These guidelines apply to all components of an information system that process, store, or transmit Federal information (NIST 2005).
OCTAVE	OCTAVE is a self-directed information security risk assessment process developed by Carnegie Mellon University and sponsored by DOD. The main objective of this standard is to assist organizations in improving their ability to manage information security risks and protect themselves from cyber threats (Software Engineering Institute, Carnegie Mellon University, 2001).

Appendix 4: IT Sector-Related Protective Programs

Table A4-1 presents brief descriptions of some of the existing protective programs (primarily Federal) that support the overarching IT Sector goals. Numerous other protective programs across the private sector; Federal, State, regional, local, and tribal government; and other organizations also enhance the physical, cyber, and human security of the sector.

Table A4-1: Existing Protective Programs that Support the Overarching IT Sector Goals

Protection/Prevention	
Protective Program	Program Description
Vulnerability Reduction	
Common Vulnerabilities and Exposures (CVE)	A mechanism for standardizing names for vulnerabilities and other information security exposures.
DHS Control Systems Security Initiative	DHS sponsors programs to increase the security of control systems. ³⁸ The DHS Control Systems Security Initiative provides coordination among Federal, State, local, and tribal governments, as well as control system owners, operators, and vendors to improve control system security within and across all CI/KR sectors.
DHS Strategic Homeland Infrastructure Risk Assessment (SHIRA)	SHIRA is designed to represent the status of vulnerability in the Nation's infrastructure.
NIST National Vulnerability Database (NVD)	NVD is a comprehensive cyber security vulnerability database that integrates all publicly available U.S. Government vulnerability resources and provides references to industry resources. It is based on the CVE vulnerability naming standard.
US-CERT Malicious Code Analysis Program	This program includes: (1) a laboratory for analyzing malicious code and developing countermeasures, and (2) a CVE dictionary system to correlate information across vendor products.
Threat Assessment	
DHS HITRAC	HITRAC conducts integrated threat analysis for CI/KR within the DHS. HITRAC brings together intelligence and infrastructure specialists to ensure a complete and sophisticated understanding of the risks to U.S. CI/KR, including cyber infrastructure.

³⁸ A control system is an interconnection of components (designed to maintain operation of a process or system) connected or related in such a manner as to command, monitor, direct, or regulate itself or another system. Control systems are embedded throughout the Nation's CI/KR and may be vulnerable to increasing cyber threats that could have a devastating impact on national security, economic security, public health and safety, and the environment.

Protection/Prevention	
Protective Program	Program Description
DOJ Computer Crimes and Intellectual Property Section (CCIPS)	DOJ's CCIPS is responsible for prosecuting nationally significant cases of cyber crime and intellectual property crime. In addition to its direct litigation responsibilities, the section formulates and implements criminal enforcement policy and provides advice and assistance.
FBI Cyber Crimes Division	The cyber mission is fourfold: (1) stop those behind the most serious computer intrusions and the spread of malicious code; (2) identify and thwart online sexual predators who use the Internet to meet and exploit children and to produce, share, or possess child pornography; (3) counteract operations that target U.S. intellectual property, endangering our national security and competitiveness; and (4) dismantle national and transnational organized criminal enterprises engaging in Internet fraud.
National Counterintelligence Center (NCIX)	NCIX, which serves as head of national counterintelligence for the U.S. Government, is directly responsible to the Director of National Intelligence. The NCIX facilitates and enhances U.S. counterintelligence (CI) efforts and awareness by: (1) enabling the CI community to better identify, assess, prioritize, and counter intelligence threats from foreign powers, terrorist groups, and other non-state entities; (2) ensuring the CI community acts efficiently and effectively; and (3) providing for the integration of all U.S. counterintelligence activities.
Community Acquisition Risk Center (CARC)	CARC performs threat analysis and risk methods/tools for Federal agencies. Also performs a threat analysis of foreign commercial entities that seek commercial relations with U.S. intelligence agencies.
US-CERT	US-CERT, established in 2003 to protect the Nation's Internet infrastructure, coordinates defense against and responses to cyber attacks across the Nation. US-CERT collaborates with Federal agencies, the private sector, the research community, State and local governments, and international entities. By analyzing incidents reported by these entities and coordinating with national security incident response centers responding to incidents on classified and unclassified systems, US-CERT disseminates actionable cyber security information to the public. US-CERT carries out numerous activities: - Maintains 24/7 Secure Operations Center; - Acts as a trusted third-party to assist in the responsible disclosure of vulnerabilities; - Develops and participates in regional, national, and international level exercises; - Supports forensic investigations with recursive analysis on artifacts; - Provides malicious software (malware) analytic and recovery support for government agencies; - Provides behavior techniques for dynamic and static analysis; - Manages the malicious code submission and collection program; - Disseminates emerging cyber threat warnings; - Administers the National Cyber Alert System to disseminate cyber security information to all Americans; - Provides fused current and predictive cyber analysis based on situational reporting; - Provides on-site incident response capabilities to Federal and State government departments and agencies; - Supports ongoing Federal law enforcement investigations; - Coordinates Federal programs of computer emergency response team and Chief Information Security Officer peer groups for sharing incident information, best practices, and other cyber security information; and - Collaborates with domestic and international computer security incident response teams.

Protection/Prevention	
Protective Program	Program Description
United States Secret Service (USSS) Electronic Crimes Task Force (ECTF)	ECTFs provide interagency coordination on cyber-based attacks and intrusions. At present, 15 ECTFs are in operation, with an expansion planned.
USSS National Threat Assessment Center (NTAC)	NTAC was created to provide leadership and guidance to the emerging field of threat assessment. Specifically, NTAC offers timely, realistic, useful, and effective advice to law enforcement and other professionals and organizations with responsibilities to investigate and/or prevent targeted violence.
Modeling and Simulation	
NCS/National Coordinating Center for Telecommunications / Network Design and Analysis Center (NDAC)	NDAC is a modeling and analysis tool designed to view the public switched network (PSN) (including the public switched telephone network (PSTN), Internet Protocol (IP), next generation packet networks, and wireless and satellite infrastructures) under various stress conditions. NDAC software resources include the tools, models, and telecommunications databases used to assess network performance, perform modeling and simulation, and visualize network topologies.
National Infrastructure Simulation and Analysis Center (NISAC)	NISAC is a joint program with Sandia National Laboratories that provides modeling, simulation, and analysis of critical infrastructures, their interdependencies, complexities, and the potential consequences of disruptions.
High Assurance Products and Services Programs	
Air Force Research Laboratory Anti-Tamper—Software Protection Initiative (AT-SPI)	The AT-SPI Technology Office is charged with developing technologies to prevent/delay the exploitation of critical program information. Of particular concern is the need to protect critical design elements or manufacturing processes. Anti-tamper technology development efforts must balance the need to protect critical technologies from exploitation, with the need to minimize the impact of anti-tamper technology application on system performance, operations and maintenance, and cost.
DHS Software Assurance Program	The DHS is leading a Software Assurance Program that addresses processes, technology, and acquisition throughout the software life cycle to result in secure and reliable software that supports critical mission requirements.

Protection/Prevention	
Protective Program	Program Description
NSA Information Assurance Directorate (IAD) Capabilities Presentations Commercial Off-the-Shelf (COTS) Product Evaluations Communications Security Evaluation Programs Controlled Cryptographic Item Agreement Global Information Grid Independent Research and Development Program IA Courseware Evaluation Program IA Outreach Information Systems Security INFOSEC Assurance Training and Rating Program National Information Assurance Partnership (NIAP)	NSA's IAD is dedicated to providing information assurance solutions that will keep our information systems safe. IAD's mission involves detecting, reporting, and responding to cyber threats; making encryption codes to pass information securely between systems; and embedding information assurance (IA) measures directly into the emerging Global Information Grid. NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) for IT security. CCEVS is a partnership between the public and private sectors. This program is being implemented to help consumers select COTS IT products that meet their security requirements and to help manufacturers of those products gain acceptance in the global marketplace.

Situational Awareness	
Protective Program	Program Description
Tactical Indications, Analysis, and Warning	
DHS Common Operating Picture (COP)/Common Operating Database (COD)	The DHS is currently developing a COP system, a situational awareness application for crises to facilitate effective information sharing and decisionmaking, and rapid staff actions. The COP is a display of relevant information that is derived from a COD and is shared by multiple agencies and organizations. Accessible through HSIN, the COP/COD system will provide a common operating database for interagency crises information sharing to ensure a common understanding of the situation and facilitate timely, risk-mitigated decisionmaking. The COP/COD system is a Web-served mission application that does not require participants to install any additional hardware or software. The DHS components and interagency partners will access the COP/COD through the HSIN; leverage the shared interagency operational database, and integrate functional and analytical tools into their operations as needed. The COP/COD system includes functional screens that address national and international situation summaries, executive actions, RFIs, blue force status, chronology, critical infrastructure, geospatial representations specified by the user, media monitoring products, video products from the field, functional metrics, and HSIN information linkages. Currently, the COP/COD development efforts have focused on preparing for the 2006 hurricane season and implementation in the selected DHS offices, and component and interagency operation centers. Subsequently, the COP/COD system will be implemented in the additional DHS component and interagency operation centers and will serve as a key information-sharing tool during crisis situations.

Situational Awareness	
Protective Program	Program Description
FBI/DHS Cyber Incident Detection Data Analysis Center (CIDDAC)	CIDDAC provides voluntary automated incident reporting to law enforcement when security breaches occur, while protecting the identity and privacy of its members and their data. CIDDAC is a nonprofit organization that integrates private, public, and government cooperation to facilitate the real-time sharing of cyber attack data.
International Watch and Warning Network (IWWN)	The IWWN consists of cyber security policy, computer emergency response, and law enforcement participants from 15 countries. The IWWN will provide a mechanism for participating countries to share information to build global cyber situational awareness and coordinate incident response.
US-CERT Einstein Program	Program is designed to build cyber-related situational awareness. It provides an automated process for collecting, correlating, analyzing, and sharing computer security information across the Federal civilian government. This automated system facilitates flow data sharing from Federal Government agencies' Internet access gateways and analyzes associated traffic patterns and behavior and provides US-CERT and participating agencies a better cyber security view and understanding across the Federal Government.
US-CERT National Cyber Alert System	US-CERT National Cyber Alert System delivers targeted, timely, and actionable information to all citizens—computer security professionals to home computer users with basic skills—to allow them to secure their computer systems. The system identifies, analyzes, and prioritizes emerging vulnerabilities and threats. It relays computer security update and warning information to all users. Alerts are issued to subscription mailing lists as well as posted on the US-CERT Web site (www.uscert.gov).
Information Sharing / Communications Mechanisms	
FBI InfraGard	InfraGard provides a trusted forum for the exchange of knowledge, experience, and information related to the protection of our Nation's critical infrastructure from physical and cyber threats. InfraGard provides its members with unmatched opportunities to promote the physical and cyber security of their organizations through access to a trusted, national network of Subject Matter Experts (SME) from the public and private sectors, spanning from the corporate and Federal to the local level. The program further provides government stakeholders, across the Federal, State, and local levels, with access to the expertise and experience of critical infrastructure owners and operators. The more than 17,000 InfraGard SMEs are active in all 50 States and represent a cross section of critical infrastructures. InfraGard members can bring subject matter expertise to the public and private sectors by State, region, or city.
Government and NSTAC Network Security Information Exchanges (NSIE)	NSIE representatives voluntarily share information related to threats, incidents, and vulnerabilities affecting operations, administration, maintenance, and provisioning systems supporting the telecommunications infrastructure. This information includes attempted or actual penetrations or manipulations of software, databases, and systems related to critical NS/EP telecommunications. In addition, representatives share information on physical intrusions pursuant to electronic attacks on network assets.

Situational Awareness	
Protective Program	Program Description
HSIN	HSIN is a national, Web-based communications platform that enables the DHS; the SSAs; State, local, and tribal government entities; and other security partners to obtain, analyze, and share information based on a common operating picture of strategic risk and the evolving incident landscape. The network is designed to provide a robust, dynamic information-sharing capability that supports NIPP-related steady-state CI/KR protection and NRP-related incident management activities. The network also will provide information-sharing processes that form the bridge between these two homeland security missions. HSIN will be one part of the ISE called for by the Intelligence Reform and Terrorism Prevention Act of 2004; as specified in the act, HSIN will provide users with access to terrorism information that is matched to their roles, responsibilities, and missions in a timely and responsive manner. HSIN-CS is a secure, unclassified, Web-based communications system that serves as the DHS's primary nationwide information-sharing and collaboration network. HSIN-CS offers real-time chat and instant messaging capability, as well as a document library that contains reports from multiple Federal, State, and local sources. It supplies information on suspicious incidents and pre-incidents, mapping and imagery tools, 24/7 situational awareness, and analysis of terrorist threats, tactics, and weapons. HSIN provides connectivity between NOC, critical private industry, and Federal, State, and local organizations responsible for or involved in combating terrorism, responding to critical incidents, and managing special events.
IT-ISAC	IT-ISAC alerts are part of the early warning system for cyber attacks; many of the companies whose products are the foundation of the Nation's IT infrastructure are members of the IT industry ISAC. Coordinates information sharing on cyber vulnerabilities among IT companies and the U.S. Government.
MS-ISAC	The mission of the MS-ISAC is to provide a common mechanism for raising the level of cyber security readiness and response in each State and with local governments. The MS-ISAC provides a central resource for gathering information on cyber threats to critical infrastructure from the States and provides two-way sharing of information between and among State and local government.
Regional Information Sharing Systems® (RISS)	RISS is a federally funded program administered by DOJ, Office of Justice Programs, and Bureau of Justice Assistance. RISS serves more than 7,300 member law enforcement agencies in 50 States, Canada, the District of Columbia, Australia, Guam, the U.S. Virgin Islands, England, and Puerto Rico. The program consists of six regional centers that share intelligence and coordinate efforts against criminal networks that operate in many locations across jurisdictional lines. Typical targets of RISS activities are terrorism, drug trafficking, violent crime, cyber crime, gang activity, and organized criminal activities. A majority of member agencies are at the municipal and county levels; however, more than 485 State agencies and more than 920 Federal agencies also participate. The Drug Enforcement Administration; FBI; U.S. Attorneys' Offices, Internal Revenue Service; USSS; U.S. Immigration and Customs Enforcement; and the Bureau of Alcohol, Tobacco, Firearms and Explosives are among the Federal agencies participating in the RISS program.

Situational Awareness	
Protective Program	Program Description
US-CERT Portal	The US-CERT Portal is a secure, Web-based collaborative system that enables members to communicate and collaborate on a real-time, 24/7 basis about emerging cyber threats and vulnerabilities. Through a suite of tools such as secure messaging, forms, secure chat rooms, alerts, and shared libraries, US-CERT is able to disseminate information to targeted audiences. As an incident reporting mechanism, it serves as a central repository of Federal incident data, ensuring that incident reports will be cataloged, indexed, and prioritized for analysis. The portal also contains four forums on emerging threats, malware code analysis, incident response, and vulnerabilities that portal members can use to collaborate on a real-time basis as necessary. The forums provide an opportunity for members to discuss suspicious activity, ask for advice, post news articles, and discuss topics of interest with other members. Forums can be tailored to a specific audience or can be created so that access is granted to everyone.

Response, Recovery, and Reconstitution	
Protective Program	Program Description
National Emergency Communications	
CWIN	CWIN is a government network within HSIN that provides mission-critical connectivity and a survivable DHS capability for information sharing, collaboration, and alerting among Federal, State, and local agencies for critical infrastructure restoration when primary forms of communication are unavailable. CWIN is a communication network designed to facilitate information sharing and collaboration of critical infrastructure and cyber information, and issue immediate alerts and notifications. CWIN communities of interest include: (1) entities in the private sector vital to restoring the Nation's critical infrastructures (e.g., electrical, IT, and telecommunication), (2) entities in the Federal and State government vital to maintain government-wide connectivity with the DHS, (3) sector-specific agencies and resources, (4) State homeland security advisors, (5) emergency management centers, and (6) international partners.
Telecommunications Service Priority (TSP)	TSP provides the regulatory, administrative, and operational framework for priority restoration and provisioning of NS/EP communications circuits in the event of an emergency. Eligibility in the TSP Program extends to Federal, State, and local government, private industry, or foreign governments that have communications services supporting an NS/EP mission.
WPS	WPS provides priority commercial mobile radio service during and after emergencies for NS/EP personnel by ensuring WPS calls receive the next available radio channel during times of wireless congestion. WPS helps to ensure that key NS/EP personnel can complete critical calls by providing priority access during times of wireless network congestion to key leaders and supporting first responders. In conjunction with GETS, it provides an end-to-end solution.
GETS	GETS provides emergency access and priority processing in the local and long distance segments of the Public Switched Telephone Network (PSTN), increasing the likelihood that NS/EP personnel can complete critical calls during periods of PSTN congestion resulting from natural or manmade disasters. GETS supports Federal, State, and local government, industry, and nonprofit organization personnel in performing their NS/EP missions. GETS uses three major types of networks: major long distance networks, local networks, and government-leased networks.

Response, Recovery, and Reconstitution	
Protective Program	Program Description
Incident Management / Response Coordination	
DOD Cyber Crime Center (DC3)	DC3 was created to better address the proliferation of computer crimes within or directed at DOD. The DC3 has three main programs: DOD Computer Forensics Laboratory (DCFL), DOD Computer Investigations Training Program (DCITP), and DOD Cyber Crime Institute (DCCI).
HSOC	HSOC serves as the Nation's hub for information sharing, situational awareness, and domestic incident management. HSOC increases coordination among Federal, State, local, tribal, and private sector partners, as well as select members of the international community. Capabilities include information collection and analysis; situational awareness and incident response coordination; and development and dissemination of threat warning products.
The Internet Fraud Complaint Center (IFCC)	The IFCC's mission is to address fraud committed over the Internet. It provides a convenient, easy-to-use reporting mechanism that alerts authorities of a suspected criminal or civil violation. It also offers a central repository for complaints related to Internet fraud.
National Cyberspace Security Response System/Program Government Forum of Incident Response and Security Teams (GFIRST) Internet Disruption Working Group (IDWG) NCRCG US-CERT: North American Incident Response Group	GFIRST, established by the DHS, facilitates interagency information sharing and cooperation across Federal agencies responsible for cyber system readiness and response. Members work together to understand and manage computer security incidents, and encourage proactive and preventive security practices. The IDWG, which was established by the DHS in January 2005, is a strategic partnership to assist the NCRCG, the US-CERT, and the private sector to coordinate contingency plans for recovering Internet functions in the event of a cyber-related incident. This working group collaborates with major security partners to identify and prioritize the short-term protective measures necessary to prevent major disruptions of the Internet or reduce their consequences, and to identify responsive/reconstitution measures for contingency plans in the event of a major disruption. The NCRCG facilitates coordination of the Federal Government's efforts to prepare for, respond to, and recover from cyber incidents and physical attacks that have significant cyber consequences (collectively known as "cyber incidents"). The NCRCG serves as the Federal Government's principal interagency mechanism for operational information sharing and coordination of the Federal Government's response and recovery efforts during a cyber crisis. It uses established relationships with the private sector and State and local governments to help manage a cyber crisis, develop courses of action, and devise appropriate response and recovery strategies. US-CERT: North American Incident Response Group (includes US-CERT, computer security incident response teams, ISACs, managed security providers, vendors, security providers, and others).
NICC	NICC is a 24/7 watch operation center that maintains operational and situational awareness of the Nation's CI/KR sectors. NICC provides a centralized mechanism and process for information sharing and coordination between and among government, SCCs, GCCs, and other industry partners. Capabilities include the following: <i>Alerts and Warnings</i> —threat-related information products to industry partners; and <i>Reporting</i> —suspicious activity and potential threats.

Response, Recovery, and Reconstitution	
Protective Program	Program Description
US-CERT Cyber Forensics Training Program (with the Computer Emergency Response Team Coordination Center) and Law Enforcement Cybercop Portal	The Cybercop Portal is a private sector initiative that is sponsored by government and industry. It is a secure Internet-based information-sharing mechanism that connects more than 8,700 members of the law enforcement community worldwide (e.g., bank investigators and the network security community) involved in electronic crimes investigations.
Contingency Planning / National Level Planning	
National Cyber Exercises	The DHS conducts exercises to identify, test, and improve coordination of the cyber incident response community, including Federal, State, Territorial, local, tribal, and international government elements, as well as private sector corporations and coordinating councils.
Top Officials (TOPOFF) Exercises	TOPOFF is a 2-year cycle of seminars, planning events, and exercises designed to strengthen the Nation's capacity to prevent, prepare for, respond to, and recover from terrorist attacks involving Weapons of Mass Destruction (WMDs). The DHS Office for State and Local Government Coordination and Preparedness (SLGCP) sponsors the TOPOFF series.
Reconstitution Plans and Programs	
NetGuard	NetGuard is a DHS-led initiative that will bring together the public sector with the State and local community following an incident that affects information systems and communications networks. The intent of the initiative is to create teams of volunteers from the private sector that could provide technical assistance and resources to the affected community. The program also could act as a clearinghouse for matching the needs of the local government and businesses with available resources in a timely manner.
Web Emergency Operations Center (WebEOC)	WebEOC is a Web-based emergency management communications system that provides cost-effective, real-time information sharing. By linking national, State, local, and even international sources, WebEOC helps to facilitate decisionmaking in emergency situations.



Appendix 5: Action Items

Section 1

Near Term (~1 year)

- Facilitate the development of and articulate for IT Sector members the national security and business value for participation in SSP implementation activities. (NCSD, SCC, and GCC)
- Develop criteria that may be used for determining nationally significant events. (NCSD, SCC, GCC, and NCRCG) (Underway)
- Provide input into national-level efforts to clarify the roles and responsibilities of public and private sectors in Federally coordinated response, recovery, and reconstitution efforts involving nationally significant events. (NCSD, SCC, GCC, and NCRCG)
- Provide public and private sector perspectives and input to assist in planning for Federally coordinated response and recovery efforts involving nationally significant events. (NCSD, SCC, GCC, and NCRCG input)

Long Term (1-3 years)

- Conduct exercises that test the implications of a nationally significant event and the resulting public and private sector roles, responsibilities, and capabilities. (NCSD, SCC, GCC and NCRCG)
- Annually review and revise IT SSP goals, objectives, and authorities. (GCC and SCC)
- Hold joint IT and Communications Sector meetings biannually to address issues of interest to both sectors, and discuss potential areas for collaboration. (NCSD, NCS, SCC, GCC, Communications SCC, Communications GCC)
- Work in partnership through the PCIS with the Communications Sector to help other CI/KR understand their dependence on the IT and Communications Sectors. (NCSD, NCS, SCC, GCC, Communications SCC, Communications GCC)

Section 2

Near Term (~1 year)

Actions to develop the IT Sector Risk Profile:

- Develop an implementation plan for the 2007 IT Sector Risk Profile. (NCSD with GCC and SCC input)
- Identify resources needed to implement the 2007 IT Sector Risk Profile. (NCSD with GCC and SCC input)

- Select the appropriate entity to manage and protect IT Sector risk management information. (SCC, IT-ISAC, and GCC)
- Decompose the sector's critical functions and/or sub-functions. (SCC, IT-ISAC, and GCC)
- Develop initial draft measurements and thresholds for consistently evaluating consequences, vulnerabilities, and threats to enable comparable risk assessment results. (SCC and IT-ISAC with GCC input)
- Initiate the identification of the sector's nationally consequential threats, and conduct analysis of them against the critical IT Sector functions. (GCC, IT-ISAC, HITRAC, and IC)
- Initiate the identification and assessment of vulnerabilities and consequences for critical IT Sector functions. (IT-ISAC with GCC input)
- Initiate the identification and assessment of mitigations that address threat, vulnerability, and/or consequences. (IT-ISAC and GCC)
- Collaborate with the Communications Sector regarding the identification and risk assessment of the Internet infrastructure, including specifically physical and cyber threat assessments for the Internet. (SCC, IT-ISAC, and GCC)

Other actions:

- Continue to encourage participation in the IT SCC and IT GCC. (SCC, IT-ISAC, and GCC)
- Encourage IT Sector entities to consider adopting individual risk management approach(es) appropriate for their unique operating environments. (SCC and IT-ISAC)
- Collaborate and coordinate with the other CI/KR sectors to address threats outside the IT Sector's control. (SCC, IT-ISAC, and GCC)

Long Term (1-3 years)

- Review (annually) critical IT Sector functions to determine if technological and environmental changes have occurred that alter the set of functions or their descriptions. (SCC and GCC)
- Identify (annually) threats, vulnerabilities, consequences, and mitigations that are of national significance to the sector. (SCC, IT-ISAC, GCC, HITRAC, and IC)
- Define and refine the IT Sector risk profile over time as the approach described in this section is implemented and repeated. (GCC, SCC, HITRAC, and IC)
- Improve cross-sector coordination. (SCC, IT-ISAC, and GCC)

Section 3

Near Term (~1 year)

- Establish the joint IT SCC and IT GCC Protective Program Working Group to review existing protective programs, identify private sector protective programs, and refine and consolidate the list of current programs. (NCSD, SCC, and GCC)
- Hold annual meeting on protective programs before developing the IT Sector CI/KR Protection Annual Report. (NCSD, SCC, and GCC)

Long Term (1-3 years)

- Raise awareness of elected and appointed officials in all branches of State government of the IT Sector's role in CI/KR protection. (NCSD with SCC, GCC, and NASCIO input)
- Report on protective program successes and lessons learned in the IT Sector CI/KR Protection Annual Report. (NCSD with SCC and GCC input)
- Conduct joint discussions with the Communications Sector on protective program effectiveness and requirements for new protective programs to avoid duplication of efforts. (NCSD, SCC, GCC, NCS, Communications SCC, and Communications GCC)
- Manage protective programs sponsored by the Federal Government in close partnership with the private sector. (NCSD, GCC, and other Federal departments and agencies)

Section 4

Near Term (~1 year)

Focal Points for Information Sharing

- Coordinate and integrate IT-ISAC and IT SCC efforts by offering recipient IT-ISAC membership to all IT SCC members and defining the roles and responsibilities of each organization to coordinate initiatives more effectively, assign accountability, and minimize duplicative efforts. (IT-ISAC and SCC)
- Increase the IT-ISAC's reach by augmenting current recruitment efforts by instituting a partnership program whereby ISAC membership is offered to representatives of IT trade associations and other IT-related organizations. (IT-ISAC and SCC)
- Identify and share POC lists to improve the ability to draw on the subject matter expertise available throughout the sector and to interact and coordinate with law enforcement for routine preparedness activities, as well as crisis situations requiring continuity of operations and continuity of government activities. (SCC, IT-ISAC, GCC, NCSD)
- Exchange information with the Communications SCC and coordinate on issues related to convergence of the IT and telecommunications infrastructures. Designating an IT SCC representative to serve on the Communications SCC and including a Communications SCC representative on the IT SCC Executive Committee will facilitate the exchange of information. (SCC)

Policies and Procedures for Sharing and Reporting Incidents

- Work with State and local governments to refine the security focus of SLFCs and clarify the relationship between SLFCs and the private sector, including clarifying how SLFCs relate to other information sharing mechanisms sponsored by DHS and how information flows between entities. (DHS and NCSD with input from SCC and GCC)
- Develop a Concept of Operations (CONOP) to formalize information sharing within the IT-ISAC's membership and between the IT-ISAC and external organizations, including US-CERT. (IT-ISAC) (Underway)
- Develop a Private Sector CONOP to guide US-CERT interaction with the private sector. (US-CERT with input from the ISAC community and other private sector security partners) (Underway)
- Develop MOUs to establish, where appropriate and necessary, formal information sharing agreements at the organizational level to better facilitate data exchange. (Individual GCC and SCC entities or other security partners as appropriate)

Procedures for Protecting and Disseminating Sensitive Proprietary Industry Information

- Raise awareness about the PCII Program among Federal, State, and local government and private sector participants and articulate the value that participants in the PCII Program can derive from submitting sensitive information. (DHS PCII Program)

- Assess the use of the PCII Program for submitting sensitive information, including risk management information, to the government. (SCC, other private sector entities, GCC, and State and local governments)

Access to Classified and SBU Government Information

- Identify private sector security partners with Federal Government issued security clearances that should receive government information, and provide their names and pertinent contact information to the DHS and other Federal departments and agencies (e.g., the IC-IRC) to facilitate more timely and extensive sharing of critical and actionable classified intelligence information with appropriately cleared individuals and organizations. (SCC, IT-ISAC, and NCSD)
- Identify mechanisms for private sector and State and local government officials who have security clearances to gain access to classified information pertinent to the IT Sector. (DHS with input from NCSD and NASCIO)

Mechanisms for Communicating and Disseminating Information

- Identify, update, and maintain appropriate private sector and State and local government POCs who should participate in emergency communication mechanisms such as CWIN, ENS, GETS, and WPS. (NCSD and NCS with SCC, IT-ISAC, and NASCIO input)
- Routinely test and exercise processes, procedures, emergency communications systems, and capabilities, document lessons learned, and make recommendations for improvement. (NCS with NCSD, SCC, and GCC input)
- Use the Homeland Security Information Network for Critical Sectors (HSIN-CS) as a mechanism for exchanging information with IT Sector private sector security partners. As information is made available, the IT-ISAC will pull it from HSIN-CS and push it to IT-ISAC members for their use. (NCSD and other components of DHS, IT-ISAC)
- Adopt a common format (e.g., ISAC Council template) for presenting information that is shared with the IT Sector private sector security partners. (NCSD working with other components of the DHS)
- Develop a strategy to leverage the Homeland Security Information Network (HSIN) to exchange IT Sector information with State and local governments. The strategy may consider duplicating or leveraging the IT-ISAC process of pulling information from HSIN-CS and pushing it to IT-ISAC members. (NCSD and other components of the DHS with NASCIO input)

Long Term (1-3 years)

Focal Points for Information Sharing

- Encourage public and private sector security partners to commit to participating in the NIPP partnership model, specifically the ISACs, including the IT-ISAC and MS-ISAC. (DHS Office of Infrastructure Protection, NCSD, NCS, and other DHS components)
- Address areas of convergence, such as those identified in the President's National Security Telecommunications Advisory Committee (NSTAC), NSTAC Report to the President on the National Coordinating Center,³⁸ including developing an approach for a long-term regional communications and IT coordinating capability that serves all regions of the Nation, convening a conference to focus on cyber issues, and exploring ideas for a multi-industry coordinating center. (NCSD, NCS, GCC, SCC, Communications SCC, Communications GCC)

Policies and Procedures for Sharing and Reporting Incidents

- Undertake an initiative to characterize and map the flow of information between and among security partners for all stages of preparedness activities. This initiative should include information on who shares what information, who receives the information, and what networks and systems are being used to disseminate and exchange the information. (NCSD and other DHS components with input from SCC, IT-ISAC, and GCC)

³⁸ President's National Security Telecommunications Advisory Committee (NSTAC), NSTAC Report to the President on the National Coordinating Center, May 10, 2006.

Procedures for Protecting and Disseminating Sensitive Proprietary Industry Information

- Develop the mechanisms and capabilities (e.g., access controls, user rights, and authentication) needed to assure the private sector that its data will be protected. (NCSD and other DHS components with input from SCC, IT-ISAC, and GCC)
- Familiarize government entities with IT-ISAC tiered information sharing mechanisms and capabilities. (NCSD and IT-ISAC)

Access to Classified and SBU Government Information

- Explore ways of clarifying the procedures for handling FOUO, SBU, LES, and other sensitive information. (Homeland Security Council with input from NCSD, SCC, and GCC)

Mechanisms for Communicating and Disseminating Information

- Design, develop, and implement a protected information sharing architecture as outlined in the NIPP. (DHS Office of Infrastructure Protection, Information Sharing Environment)
- Exercise processes and procedures (e.g., standard operating procedures and CONOPs) and communication mechanisms (e.g., HSIN-CS, GETS, CWIN, and WPS) and evaluate lessons learned to enhance information sharing from a cultural, organizational, and technological perspective. (NCSD, NCS, DHS Office of Infrastructure Protection, SCC, GCC)
- Achieving an enhanced information sharing framework requires commitment from public and private sector security partners. Participation in the IT SCC and IT GCC requires commitment not only on the part of individual members, but also on the part of the organizations employing them. Implementation of the above actions cannot be achieved without a core group of committed individuals from the public and private sectors. This core group of individuals and organizations may not necessarily be the same as those who were responsible for outlining the vision for an enhanced information sharing framework. Investment in resources and human capital is necessary for success.

Section 5

Near Term (~1 year)

- Establish an IT Sector R&D Working Group and identify opportunities for public and private sector security partners to collaborate on R&D priorities. (NCSD, S&T Directorate, SCC, and GCC)
- Brief R&D institutions listed above on the SSP to raise awareness of IT Sector R&D priorities, goals and objectives, and risk management approach. (NCSD, S&T Directorate, SCC, GCC)
- Coordinate with the Communications Sector on R&D CI/KR protection priorities that overlap or have inherent synergies. (NCSD, SCC, GCC, NCS, Communications SCC, Communications GCC)

Long Term (1-3 years)

- Plan and execute annual IT Sector R&D Workshop, and share results with R&D public and private sector security partners. (SCC and GCC)
- Develop a 5-year roadmap for IT Sector R&D priorities and resource needs. (S&T Directorate and NCSD with input from SCC and GCC)

Section 6

Near Term (~1 year)

- Update the IT SSP annually. (GCC and SCC)
- Develop (annually) the IT Sector CI/KR Protection Annual Report. (NCSD with GCC and SCC input)
- Identify necessary resources to implement the IT SSP risk management approach, protective programs, information sharing mechanisms, R&D initiatives, and performance measurement. (NCSD, GCC, and SCC)
- Engage with and develop public sector programs to support the implementation and maintenance of the IT SSP. (NCSD)
- Coordinate closely with the Communications Sector on the development of the next Communications SSP. (GCC and SCC)

Long Term (1-3 years)

- Develop and facilitate training and education initiatives necessary to implement the IT SSP successfully. (NCSD, GCC, and SCC)
- Collaborate with the Communications Sector on outreach and education to customers on their reliance on Communications and IT infrastructures and security roles and responsibilities. (NCSD, GCC, SCC, NCS, Communications SCC, Communications GCC)
- Fulfill the roles and responsibilities identified in section 6.3. (All)

Section 7

Near Term (~1 year)

- Prioritize sector action items, taking into consideration available resources. (NCSD, SCC, GCC)
- Create Gantt chart for the sector that maps SSP actions to objectives and goals. (NCSD with input from SCC and GCC)

Long Term (1-3 years)

- Continue to reassess action item prioritization based on evolving status of the sector and resource availability. (NCSD, SCC, and GCC)
- Track sector action item progress and update the IT SSP. (NCSD, SCC, and GCC)





Homeland
Security

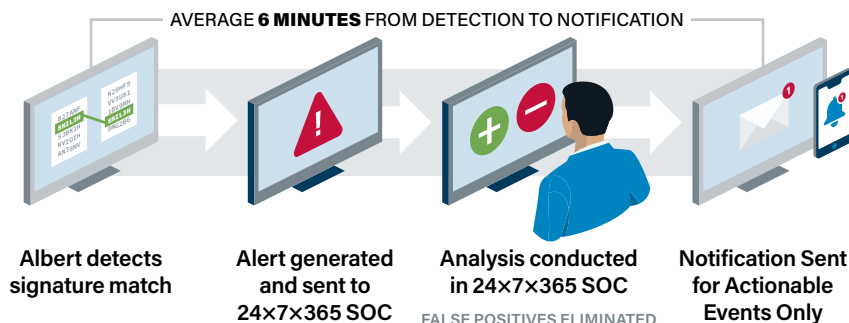
Albert Network Monitoring and Management

The Center for Internet Security, Inc. (CIS) offers a fully managed network security monitoring service called Albert. Albert is available to U.S. State, Local, Tribal, and Territorial governments, including elections entities, critical infrastructure, and public education. Albert can be used to monitor many types of traffic including networks with user workstations, web servers, or those hosting voter registration databases. Albert has the flexibility to monitor traffic at the edge and internally.

Albert provides network security alerts for both traditional and advanced network threats, helping organizations identify malicious and anomalous activity. This cost-effective Intrusion Detection System (IDS) uses open source software combined with the expertise of the CIS 24x7x365 Security Operations Center (SOC) to provide enhanced monitoring capabilities, cyber threat intelligence, and notifications of malicious activity, including full management of the device.

How Does Albert Work?

Albert looks for malicious activity by comparing network traffic to signatures that detect known malicious and anomalous activity. When a match is found, expert SOC analysts review for malicious activity and alert the customer of any valid threats. The basic lifecycle of an Albert event is as follows:



An IDS is only as effective as the signature set running on it. Albert utilizes a unique SLTT-focused and targeted signature set to ensure sensors rapidly recognize and alert on potentially malicious traffic occurring on the network.

Signatures and indicators of compromise.

Albert utilizes commercial, open-source, and custom signatures developed from leveraging our federal partners for access to recently declassified signatures, indicators CIS derives from incident response cases, as well as member submitted and third-party threat data.



Commercial Signatures



Recently Declassified Signatures



CIS Research – Threat Data Analysis CIRT Cases

Services Provided with Albert

- 24x7x365 network monitoring from the CIS SOC (U.S.-based)
- Alerts about potentially malicious activity
- Monthly activity summary reports

Additional Data We Collect

We collect data about the traffic, not what's in the traffic, in addition to alert data about the signatures firing.

- 1 Source IP
- 2 Destination IP
- 3 Source port
- 4 Destination port
- 5 TCP flags
- 6 Number of bytes of traffic sent and received
- 7 Timestamp information (start, end, and duration of connection)

Data can be analyzed in real time or retroactively through a query.

To find out more about network security monitoring, contact us today at services@cisecurity.org

"I now have a reliable, affordable, and trusted source that inspects ALL of my traffic in both directions."

Wesley Wilcox
Marion County, Florida Elections

For Questions

services@cisecurity.org
www.cisecurity.org
518-880-0699



Albert Network Monitoring Options

Organizations can opt to deploy more than one Albert sensor for high availability and can have them as an active/active or active/passive configuration.

	ALBERT ON-PREMISES
SENSOR TYPE	Physical sensor on your network
WHAT IT MONITORS	Monitors traffic on your on-prem network
SCALABLE BASED ON TRAFFIC	Yes
ALERTS ANALYZED BY CIS SOC	Yes

Pricing

The annual fee covers both the management and monitoring of Albert. CIS also offers a turnkey solution, which includes hardware.

Pricing is based on average internet connection utilization. A one-time initiation fee of \$900 per sensor applies.

AVERAGE UTILIZATION	CUSTOMER-PROVIDED HARDWARE			HARDWARE INCLUDED	
	ANNUAL FEE (USD)	PER MONTH	PER DAY	ANNUAL FEE (USD)	PER MONTH
0MB-100MB	\$10,680	\$890	<\$30	\$13,080	\$1,090
101MB-1.0GB	\$13,800	\$1,150	<\$38	\$16,200	\$1,350
1.01GB-5.0GB	\$25,200	\$2,100	<\$70	\$28,800	\$2,400
5.01GB+	Please contact services@cisecurity.org for more details.				

For More Information

To find out more about network security monitoring, contact us today at services@cisecurity.org.



Center for Internet Security, Inc.
31 Tech Valley Drive
East Greenbush, New York 12061
United States

ORDER for City of Alpharetta
Order: SO-220826-0034542
Created Date: 8/26/2022
Valid Through: 12/24/2022
Prepared by: Todd Dusse
Phone: (518) 516-6132

Order

Address Information

Bill To:

City of Alpharetta
2 Park Plaza
Alpharetta, Georgia 30009
United States

Buying Contact: ADAM MONTGOMERY

Buying Email: amontgomery@alpharetta.ga.us

Ship To:

City of Alpharetta
2 Park Plaza
Alpharetta, Georgia 30009
United States

Shipping Contact: ADAM MONTGOMERY

Shipping Email: amontgomery@alpharetta.ga.us

Related Information

Currency: USD

Billing Frequency: One-Time

Product Lines

Product	Product Code	Date	Qty	Term	List Price	Sales Price	NET
CIS Albert MD Appliance Primary Sensor Initialization	CIS-ALB-MD-APP-PR-O-A	8/1/2022	2 Each		\$900.00	\$900.00	\$1,800.00

Service Lines

Service	Product Code	Date	Qty	Term	List Price	Sales Price	NET
CIS Albert MD Appliance Primary Sensor	CIS-ALB-MD-APP-PR-M-A	8/1/2022 - 7/31/2023	2	12 Mon	\$1,350.00	\$1,350.00	\$32,400.00

List Price Total: \$34,200.00

Sales Price Total: \$34,200.00

Net Amount: \$34,200.00

Balance Due Amount: \$34,200.00

Standard Terms

Please note that if the purchase(s) listed above are related to a new product/service, the Date(s) are determined based upon both the order being approved and all pre service requirements met. If the purchase(s) listed above are for a renewing product/service, the Date(s) reflect the actual term.

The fees are listed in USD and do not include any taxes (including but not limited to VAT or withholding taxes) or fees to be collected by a taxing jurisdiction, financial institution or payment processor incidental to the payment of the Balance Due Amount. If Customer is located in a country with applicable VAT/Withholding taxes, Customer is required to declare and make the VAT/Withholding payment. Once Customer makes the required VAT/Withholding payment, a copy of the receipt will be provided to CIS for our records.

Your acceptance of this Order shall constitute your intent to proceed with the purchase of the product or service listed above.

Customer: City of Alpharetta

Signature

Name

Title

Date

All rights reserved. Copyright Center for Internet Security, Inc.



STAFF REPORT

Submitting Department: Community & Economic Development

Submitted By: Kathi Cook

Sponsored By:

Meeting Date: September 26, 2022

I. AGENDA ITEM TITLE: WINDWARD / HIGHWAY 9 AREA STRATEGIC MASTER PLAN
APPROVAL OF AUTHORIZING FUNDING IN AN AMOUNT TOTALING \$60,000 TO PARTICIPATE IN THE WINDWARD/HIGHWAY 9 MASTERPLAN LCI UPDATE STUDY IN PARTNERSHIP WITH THE NORTH FULTON CID AND THE CITY OF MILTON.

II. RECOMMENDATION:

Authorize funding in an amount totaling \$60,000 to participate in the Windward/Highway 9 Masterplan LCI update study in partnership with the North Fulton CID and the City of Milton.

III. BUDGET IMPLICATIONS:

BUDGETED ITEM: NO

FISCAL IMPACT: YES

INCLUDED IN CURRENT FY CPTL BUDGET: NO

INCLUDED IN CURRENT
FY OPRT. BUDGET: NO

TOTAL PROJECT COST: \$60,000. INCLUDED IN THIS FUNDING REQUEST IS A REALLOCATION OF \$60,000 FROM THE NON-ALLOCATED RESERVE ACCOUNT WITHIN THE CAPITAL PROJECT FUND LEAVING AN ESTIMATED BALANCE OF \$2.3 MILLION.

APPROPRIATIONS:

<u>ACCOUNT TITLE/NUMBER</u>	<u>DOLLAR AMOUNT</u>
Non-Allocated Reserve Reallocation (Capital Project Fund; 30190200-579000)	\$60,000

EXTERNAL FUNDING SOURCES:

<u>ACCOUNT TITLE/NUMBER</u>	<u>DOLLAR AMOUNT</u>
N/A	\$0.00

IV. REPORT IN BRIEF:

In February of 2022 Council approved a resolution authorizing staff to apply to the Atlanta Regional Council (ARC) for a Livable Centers Initiative (LCI) grant in cooperation with the City of Milton and the North Fulton Community Improvement District (NFCID) to update the 2012 Windward/Highway 9 Master Plan. ARC notified the NFCID that our grant was not funded. NFCID has taken the lead and asked both cities to participate in funding the update with the cost split between the 3 parties. The NFCID estimates the total project cost from \$150,000 - \$180,000 and requests a maximum of \$60,000 from City of Alpharetta and the same from City of Milton.

If this \$60,000 funding request is approved, Staff will work with the parties and the City Attorney to draft an appropriate MOU that addresses the specifics of how costs would be shared, funds paid, and other important details. That MOU would then be presented for consideration during a future City Council Meeting.

Created as a way to reduce vehicle miles traveled and improve air quality, the ARC LCI is a grant program that incentivizes local jurisdictions to re-envision their communities as vibrant, walkable places that offer increased mobility options, encourage healthy lifestyles, and provide improved access to jobs and services. The City of Alpharetta partnered with the City of Milton in 2011 to complete an LCI Study for the Windward/Highway 9 area. A plan was adopted in 2012 and it details a vision for the future of the study area based on a thorough planning process that included input from community leaders, a Core Team of stakeholders, and a series of public workshops.

The plan includes a 5-Year Action Plan consisting of short-term and long-term projects and other initiatives to enhance land use, economic development, and mobility within the area. Recommendations ranged from the identification of character areas and encouraging mixed-use development to specific vehicular and pedestrian connections. While progress has been made as a result of the 2012 LCI including new development regulations in Milton and improvements to Windward Parkway in Alpharetta, significant change has occurred in the Windward Parkway/Highway 9 area over the last 10 years. The changing economic market, consumer demands, and new mobility opportunities necessitate review of challenges and opportunities that impact development patterns and mobility investments.

As a corridor planned to receive a BRT station related to the GA 400 MMIP (Major Mobility Investment Program) project, as well as with current development trends moving away from big box stores and separated land uses, the Windward Parkway corridor/Highway 9 area requires an updated community vision and action plan achievable through the 10-Year LCI Study Update.

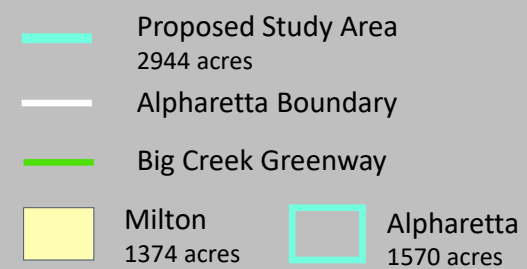
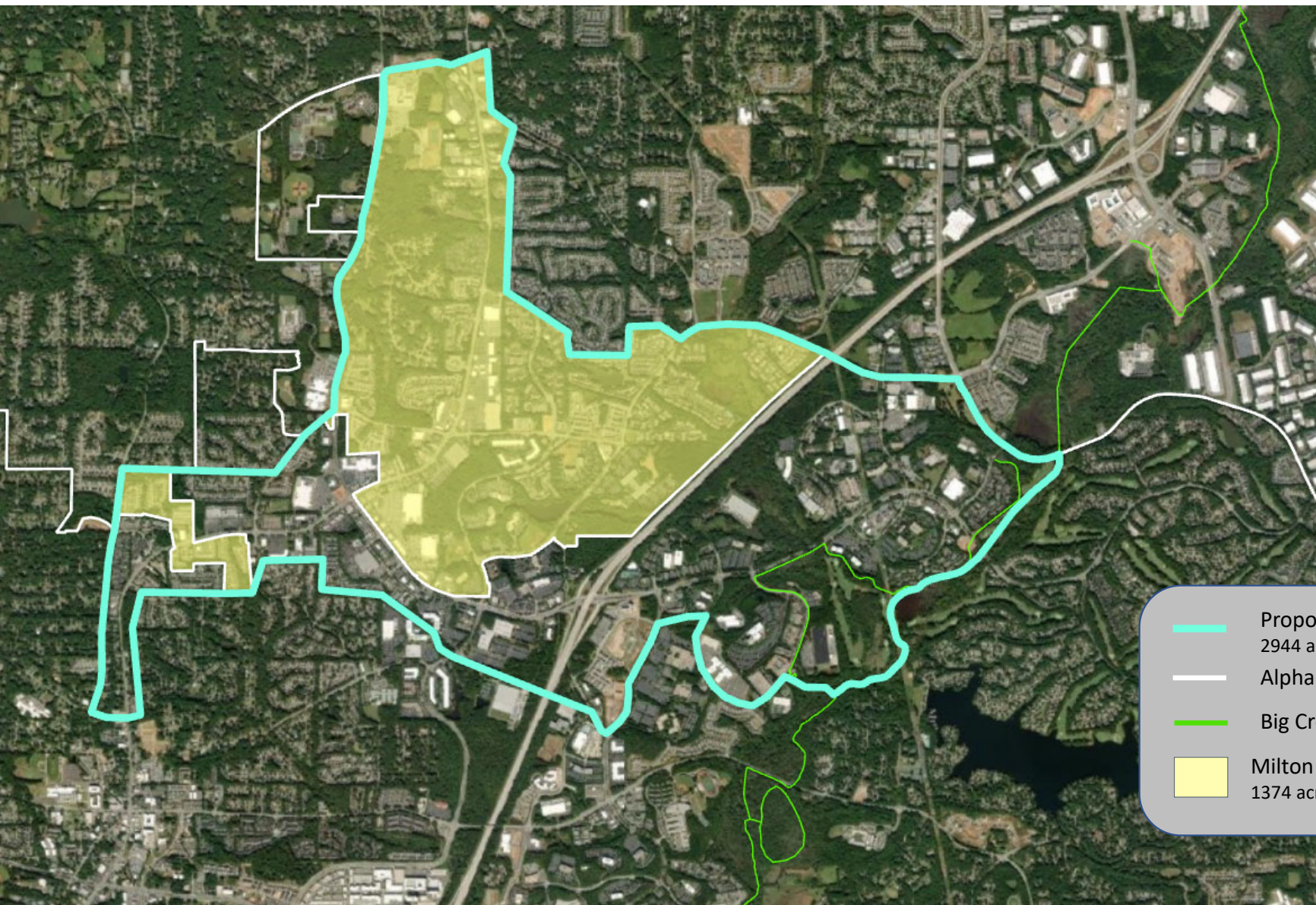
Potential outcomes of this LCI Study Update will include:

- An updated market study and branding strategy for the area
- Strategies for integrating the planned BRT station and providing first/last mile connectivity
- An updated approach to land use and transportation that evolves the area from a place centered around the automobile to a walkable transit-supported place

V. ALTERNATIVES:

VI. ATTACHMENTS:

Windward Master Plan Total+City Area+Proposed, WindwardHighway9_Scope_Budget_Draft_2022-09-02



Windward/Highway 9 Area Strategic Master Plan

While progress has been made as a result of the 2012 Windward/Highway 9 LCI, including new development regulations in Milton and improvements to Windward Parkway in Alpharetta, significant change has occurred in the Windward area over the last 10 years. The changing economic market, consumer demands and preferences, and new mobility opportunities necessitate a fresh look at the challenges and opportunities that impact development patterns, community development, and mobility investments in the Windward/Highway 9 Area. As a corridor planned to receive a high-capacity transit station related to the GA 400 Express Lane project, as well as current development trends moving away from big box stores and separated land uses, the Windward/Highway 9 Area requires an updated community vision and action plan.

This document proposes a Strategic Master Plan effort as the mechanism through which to accomplish these goals, with the following anticipated outcomes and deliverables:

- A tool to inform current and future stakeholders about the **NFCID and Cities of Alpharetta and Milton's collective vision and goals for the area**
- An **updated approach to land use and transportation integration** that evolves the area from a place centered around the automobile to a more walkable, multimodal transit-supportive place
- Strategies **for integrating the planned high-capacity transit station** and providing **first/last mile connectivity**
- An **updated market study** to assist developers in gaining an understanding of the type, scale, design and location of desired development
- A **branding strategy** for the area that re-creates it as a destination and improves sense of place
- An updated **5-year Action Plan** of projects and initiatives, with a **heavy focus on the identification of follow-up/supplemental studies, projects, and initiatives** that are ready for future funding opportunities

The Strategic Master Plan will focus on both Windward Parkway and Highway 9 as central corridors positioned for future project efforts and investments. Specific to Windward Parkway is its future character and identity, development, and connectivity to the planned high-capacity transit station, while for Highway 9 an emphasis on the repositioning of older retail parcels and big box developments is anticipated to present opportunities for future reinvestment.

SCOPE SUMMARY

Task 1- Existing Plan Assessment

The process will begin with a **kick-off meeting with the Project Management Team (PMT)**. The PMT will be comprised of representatives from the NFCID, Cities of Alpharetta and Milton, and the Consulting Team. The kick-off meeting will include review of the most recent LCI 5-year action plan, activities in and around the area since the original plan and last update, a discussion of plan goals and objectives, and review of the project schedule and communication protocols.

Following the kick-off meeting, the consulting team will review the original LCI Plan and 5-year update, other relevant planning documents including recently updated Comprehensive Plans, and any other area land use, transportation, or

market studies; review recent development proposals and activity; and conduct an updated review of existing conditions including area land use, transportation, and market trends and fundamentals.

The consulting team will review existing plan assessment findings with the PMT and assist the NFCID in identifying members for the Core Team of area representatives. An overview of the assessment will be presented to and discussed with the **Core Team** and then prepared for communication to area stakeholders and the public.

Upon completion of the Existing Plan Assessment Summary, the consulting team will facilitate a **public workshop or event** to help update the plan's vision, goals, and objectives. Public Workshop #1 will include a presentation of the planning process and existing plan assessment and include a variety of interactive exercises to engage area leaders, landowners, businesses, employees and stakeholders in refining the vision for the future of the Windward/Highway 9 Area.

Task 1 Meetings:

- Kick-off Meeting with PMT
- Core Team Meeting #1
- Public Meeting #1

Task 1 Milestones/Deliverables:

- Existing Plan Assessment Summary

Task 2- Market Analysis

Following the existing plan assessment and concurrent with the first Core Team Meeting and Public Workshop #1, the consulting team will conduct a **market analysis of the Windward/Highway 9 Area**. After identifying an appropriate Windward/Highway 9 trade area, the team will review demographic information and trends, customer profiles, and the level of market opportunity by land use and product type. The analysis will include an assessment of competing retail, office, and employment districts; a projection of retail, office, and employment feasibility over the next 5 and 10 years; and estimate housing potential by residential type.

A **summary presentation** of the market analysis will be reviewed with the PMT and presented to the **NFCID Board** along with relevant project findings to-date.

Task 2 Meetings:

- Market analysis review with PMT
- Market Summary NFCID Board Presentation

Task 2 Milestones/Deliverables:

- Market Summary Document

Task 3- Plan Development

The identification of concepts and strategies to enhance the Windward/Highway 9 Area will begin with an **opportunity assessment**, an identification of obstacles and opportunities to enhance connectivity, walkability, and placemaking in the Windward/Highway 9 Area and to leverage the future planned high-capacity transit station at Windward Parkway and GA 400.

As part of or closely following the opportunity assessment, the consulting team will facilitate **Core Team Meeting #2**. The Meeting will include a review of findings and a discussion of opportunities to enhance the Windward/Highway 9 Area.

Based on the input analysis completed to date and gleaned from best practices in other, similar locations – as well as feedback from plan participants, the Team will develop preliminary concepts related to land use, transportation, walkability, and placemaking. The Team will also develop a preliminary list of improvement projects and initiatives for review with the PMT and the Core Team at **Core Team Meeting #3**.

With input from the PMT and Core Team, the consulting team will review **preliminary concepts and project lists** and prepare them for property owner and community member outreach and input.

Task 3 Meetings:

- Core Team Meeting #2
- Concept review meeting with PMT
- Core Team Meeting #3

Task 3 Milestones/Deliverables:

- Opportunity assessment summary and graphics
- Preliminary land use and transportation concepts and project lists

Task 4- Action Plan/Implementation

The consulting team will develop a **Draft 5-Year Action Plan** as well as **recommended additional studies and plan funding strategies**.

The Team will assist in conducting up to **2 Focus Group Sessions with property owners in the area** to identify first steps and incentives that would better enable area property owners to reinvest or redevelop key properties in a manner consistent with plan goals and objectives. The Team will schedule meetings with appropriate ownership groups, gather input, and discuss plan or action item modifications with the Client based on the opportunities and constraints for key sites and parcels. This will be followed by **City Staff and Elected Officials Engagement Sessions** to gather input related to the Draft 5-year Action Plan.

The Team will then schedule a **NFCID Board Work Session** to further refine the Draft 5-year Action Plan and review input from the focus group sessions.

Following this, the consulting team will facilitate **Public Workshop #2** to provide an opportunity for area stakeholders to help review and prioritize action items and implementation initiatives. Results from this public workshop will be reviewed with the PMT and at **Core Team Meeting #4**.

With the input of the Core Team, the consulting team will prepare a **summary of plan recommendations** and an outline for the draft document. Recommendations and summaries will provide the foundation for a **plan review and transportation coordination meeting with ARC**, with a focus on action and implementation items that may benefit from ARC input, assistance, or future funding.

The **draft document** will be provided to the PMT for review and comment. The draft document will include:

- Overview of existing conditions and the plan development process
- Market analysis

- Updated concept plans
- 5-Year Implementation Plan

The consulting team will make one round of revisions and present the Draft Document to City Councils and the NFCID Board for review and adoption.

Task 4 Meetings:

- Action Plan review with PMT
- Focus Group Sessions: Major property owners
- Focus Group Session(s): City Staff and Elected Officials
- NFCID Board Work Session
- Public Workshop #2
- Follow up meeting with PMT
- Core Team Meeting #4
- City Councils and NFCID Board review and adoption

Task 4 Milestones/Deliverables:

- Draft 5-Year Action Plan
- Summary of Plan Recommendations
- Draft Document
- Final Document and Deliverables

BUDGET

The proposed budget for the Windward/Highway 9 Area Strategic Master Plan is \$150,000:

Task 1 Existing Plan Assessment	\$ 32,400
Task 2 Market Analysis	\$ 32,100
Task 3 Plan Development	\$ 42,610
Task 4 Action Plan/Implementation	<u>\$ 42,890</u>

Funding Scenario

Aligned with a shared interest in undertaking this Strategic Master Plan, the following funding scenario has been contemplated among the involved entities:

Entity	Funding Responsibility
NFCID	\$50,000 – 60,000
City of Alpharetta	\$50,000 – 60,000
City of Milton	\$50,000 – 60,000

SCHEDULE

Please see the following page for associated proposed schedule.

[illegible]



STAFF REPORT

Submitting Department: Community & Economic Development

Submitted By: Charlotte Christian

Sponsored By:

Meeting Date: September 26, 2022

I. AGENDA ITEM TITLE: ECONOMIC DEVELOPMENT STRATEGIC PLAN KICKOFF PRESENTATION

II. RECOMMENDATION:

No formal action by City Council is being requested. The purpose of this item is to present the anticipated program of work and receive input and feedback from City Council.

III. BUDGET IMPLICATIONS:

BUDGETED ITEM: NO

FISCAL IMPACT: NO

INCLUDED IN CURRENT FY CPTL BUDGET: NO

INCLUDED IN CURRENT FY OPRT. BUDGET: NO

TOTAL PROJECT COST:

APPROPRIATIONS:

<u>ACCOUNT TITLE/NUMBER</u>	<u>DOLLAR AMOUNT</u>
-----------------------------	----------------------

EXTERNAL FUNDING SOURCES:

<u>ACCOUNT TITLE/NUMBER</u>	<u>DOLLAR AMOUNT</u>
-----------------------------	----------------------

IV. REPORT IN BRIEF:

In December 2019, the City awarded RFP 20-112 (Economic Development Strategic Plan) to RKG Associates, Inc. Funding for the development of the plan was split between the City (\$43,890) and the Alpharetta Development Authority (\$37,500). A contract was subsequently awarded, and work began, with an anticipated completion of June 2020.

Work on the plan was halted in March 2020 due to the COVID-19 pandemic and its impacts on businesses and the economy.

The purpose of the Economic Development Strategic Plan is to position the City and its public, private, and institutional partners on a path that continues to act upon opportunities to drive investment and economic growth. A completed version of the plan will include best practices for business retention and expansion, recommendations for maximizing the City's entrepreneurial and small business ecosystem, strategies for leveraging existing employment centers and commercial nodes, identification of incentive programs that will help attract and retain job growth in targeted industries, and identification of strategies that will guide key corridors to reach their maximum economic potential.

It is now time to restart the effort to develop a new Economic Development Strategic Plan. A new project steering committee has been constituted, and work is ready to begin.

During the September 26, 2022, City Council Meeting, members of our economic development staff and representatives of our consulting team will provide an overview of the work ahead and formally launch the planning process. This presentation was previously an item on the agenda of the June 20th council meeting but was tabled since the body failed to meet a quorum.

V. ALTERNATIVES:

VI. ATTACHMENTS:

ED Strategic Development Plan Presentation



Alpharetta, Georgia

KICKOFF MEETING
**Strategic Economic
Development Plan**

September 26, 2022

Presented by:
Kyle Talente, President

RKG
ASSOCIATES INC



Project Timeline

- **The project started in February of 2020**
 - Kickoff meeting with the council occurred in March of 2020
- **The City placed a stop order in April of 2020 as a result of the COVID pandemic**
 - RKG had done initial interviews, administered a community survey (ended at stop order), and completed the socioeconomic and real estate analyses
- **The project was restarted in May of 2022**
 - RKG will need to update the completed studies and will execute the remaining tasks that were not started in 2020
- **There is an expected completion date of December 2022**
 - A working group has been assembled to engage during the study
 - RKG will hold milestone meetings to present findings and strategies during the process



What is
Economic
Development?

**What does
ECONOMIC
DEVELOPMENT
mean?**

RKG Associates
Definition

Economic Development is a
series of strategic actions and
investments that leverage
public assets to attract private
investment, **improving the**
financial, fiscal, and economic
well being of the community.



How is Economic Development Success Defined?

- **Benchmarks vary greatly, but all are relevant**
 - Business attraction
 - Business retention / expansion
 - Job creation
 - Tax base development
 - Quality of life
 - Preservation
 - Entrepreneurial growth
 - Sustainability
 - Environmental enhancement
 - Tourism development
- **LOCAL PRIORITIES DEFINE SUCCESS;
FRAME IMPLEMENTATION**



What Would You Choose?

OPTION A

- **\$2,500,000** of new annual tax base
- **No** jobs

OPTION B

- **\$500,000** of new annual tax base
- **25** jobs paying **\$50,000**



What an Economic Development Plan is...

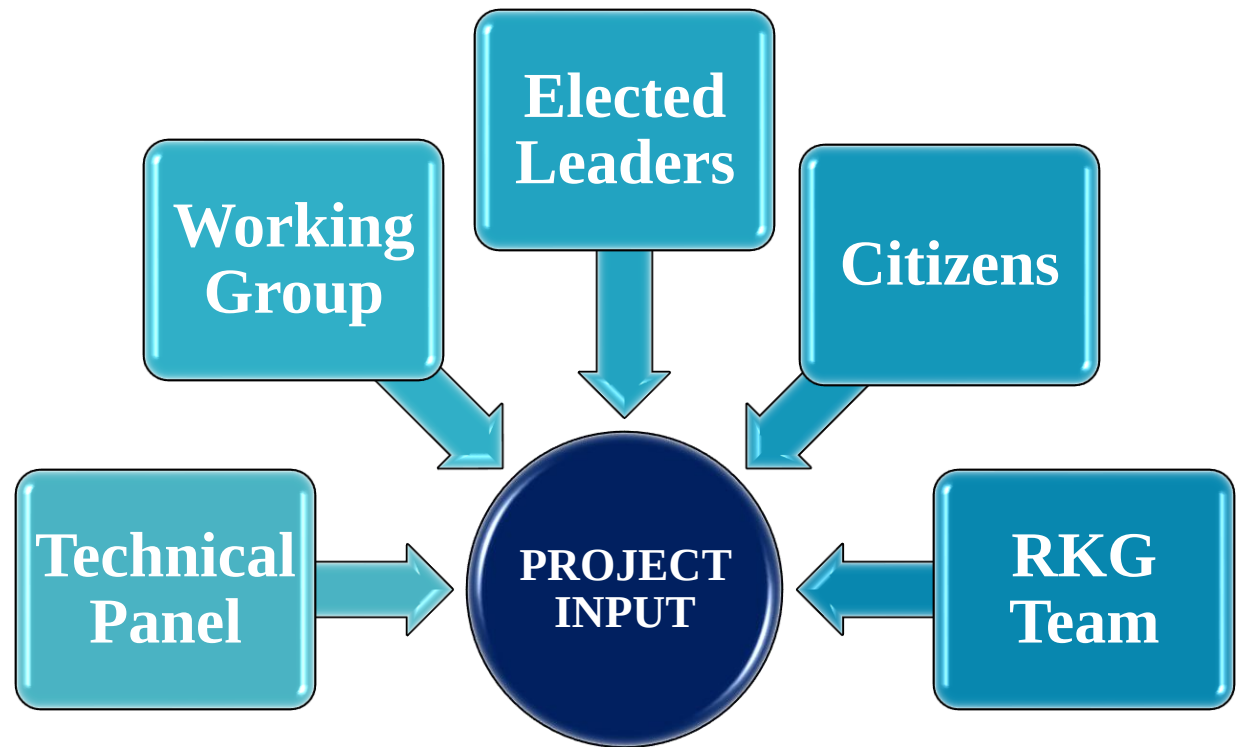
- **Baseline Analysis**
 - SWOT
 - Market Assessment
 - Public Asset Analysis
 - Workforce
 - Competitive Analysis
- **Target Industry Analysis**
 - Cluster Identification and Definition
 - Supply Chain and Logistics Industry Analysis
- **Strategic Recommendations**
 - Organization
 - Toolkit
 - Prioritization
 - Asset Management
 - Collaboration



What an Economic Development Plan is **NOT**...

- **“THE” Answer**
 - Plan must be focused, but flexible
 - Mindful of investment motivations
- **A “Cheerleader”**
 - Honest assessment of all challenges
 - For better or for worse...
- **One size fits all**
 - Concepts relevant to the local community
 - Customized to community / areas of community / vision
- **Parcel by parcel**
 - City-wide
 - Area specific
 - Context appropriate

Participation

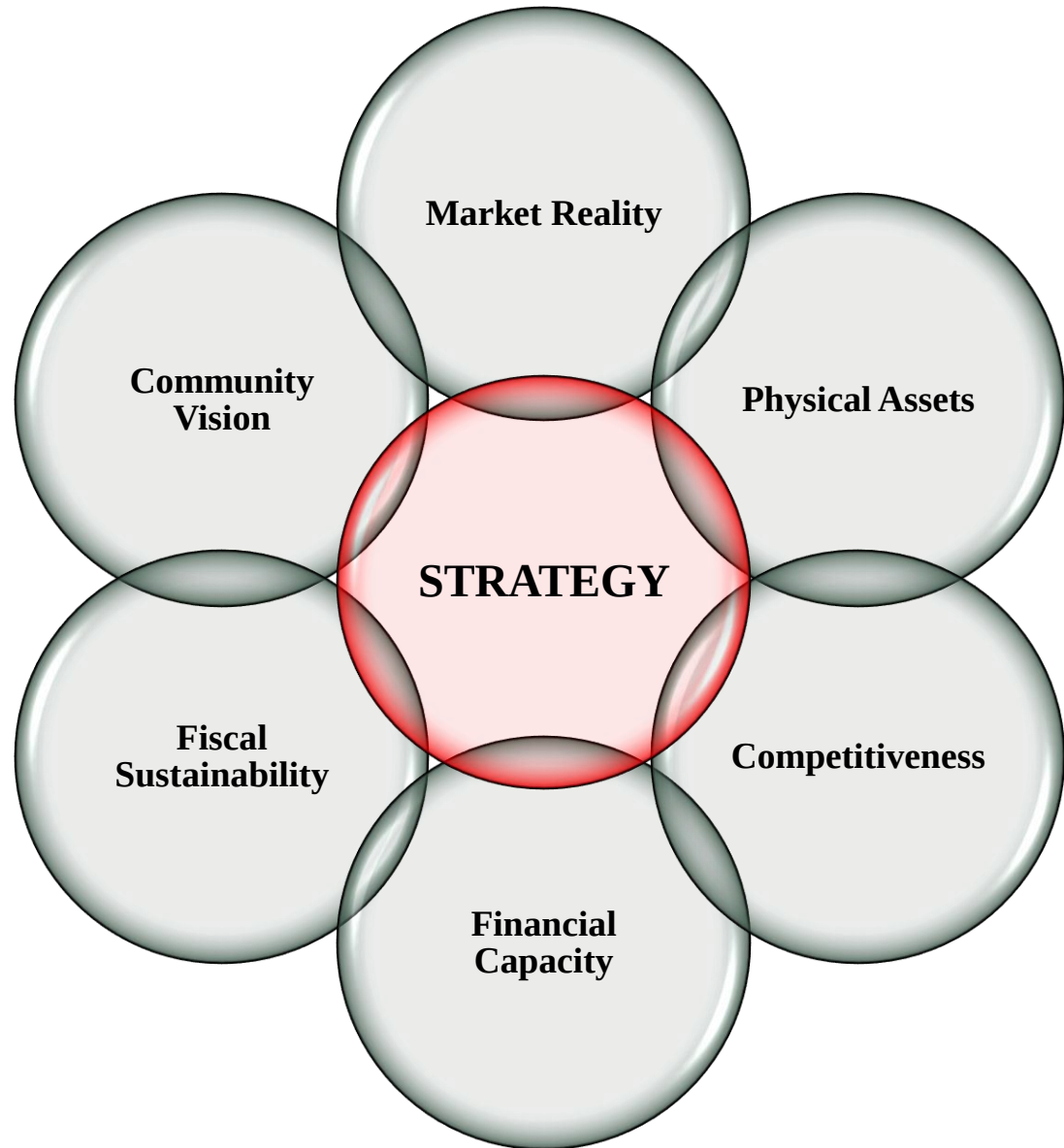




Engagement Approach

- **Technical Panel**
 - Comprised of essential staff. Continuous engagement on progress, project planning, strategic feedback and data collection
- **Working Group and Elected Officials**
 - Series of 5 meetings presenting findings and strategies at key milestones
 - Today is the kickoff meeting
- **Public**
 - 2 open house/town hall meetings to provide information and collect additional feedback

Building to Consensus



PROVIDING A ROADMAP

AN APPROACH TO ECONOMIC DEVELOPMENT PLANNING

Strategies

What do we need to do to create our impact and tell our story?

1

Capacity

Who can do this, can we do this with current staff, do we need to reorganize?

2

Funding

How can we fund this, what partners do we need, how much will this cost?

3

Timing

What needs to happen first, what are the key priorities?

4



Elected Leadership Involvement

- **Plan Development**
 - Interim briefings from staff and the consultant
 - Provide input and feedback
- **Plan Approval**
 - Approve the plan
- **Plan Implementation**
 - Familiarize with the plan contents
 - Champion the cause with constituents
 - Build (up) relationships with stakeholders
 - Enact regulatory policies consistent with goals
 - Promote unity with the message

**Discussion
Questions**

**What do you believe the economic
development goals for Alpharetta
should be?**

**Discussion
Questions**

**What opportunities/investment
areas should be focused on
during this analysis?**



Other
Thoughts?

**THANK YOU FOR YOUR
PARTICIPATION!**

**Kyle Talente
President
RKG Associates, Inc.
kst@rkgassociates.com**



What is
Economic
Development?

New Residents

Housing Diversity

TAX REVENUES

Redevelopment

JOBS

Growth

Quality of Life

Building Rehab

Traffic

New Businesses



What Would You Choose?

OPTION A

- **\$2,500,000** of new annual tax base
- **No** jobs

OPTION B

- **\$500,000** of new annual tax base
- **50** jobs paying **\$50,000**



What Would You Choose?

OPTION A

- **\$2,500,000** of new annual tax base
- **No** jobs

OPTION B

- **\$500,000** of new annual tax base
- **25** jobs paying **\$50,000**
- **Early Childhood Development Center**



What Would You Choose?

OPTION A

- **\$2,500,000** of new annual tax base
- **No jobs**
- **2-Acre Park**

OPTION B

- **\$500,000** of new annual tax base
- **50 jobs** paying **\$50,000**
- **Early Childhood Development Center**



Working Group Responsibilities

- **Plan development**

- Listening
- Learning
- Assessing
- Brainstorming
- Challenging

The Working Group informs the plan along with input from elected officials, staff, the Consultant, and input from the community.

- **Plan implementation**

- Supporting
- Championing
- Doing

- **This process is interactive**

**Discussion
Questions**

What concerns/issues should we be aware of while we do this analysis?