



City of High Point

Municipal Office Building
211 S. Hamilton Street
High Point, NC 27260

Meeting Agenda

Finance Committee

Britt Moore, Chair
Committee Members:
Monica Peters
Michael Holmes
Victor Jones

Jay Wagner, Mayor (Alternate)
Wesley Hudson, Mayor Pro Tem (Alternate)

Thursday, May 11, 2023

4:00 PM

3rd Floor Conference Room

FINANCE COMMITTEE - Britt W. Moore, Chair

CALL TO ORDER

PRESENTATION OF ITEMS

- [2023-211](#) Amendment No. 2 - GEL Engineering of NC - Eastside Wastewater Treatment Plant
City Council is requested to approve Amendment No. 2 in the amount of \$15,700 to modify the original supplemental agreement entered on July 20, 2022 (PO Number 109917) with GEL Engineering of NC for on-call air permitting assistance at the Eastside Wastewater Treatment Plant.
Attachments: [Supplemental Agreement Amendment 2– Assistance with Air Permit Reporting I](#)
- [2023-212](#) Resolution - American Rescue Plan Act Grant Funding (ARPA) - Whites Mill Pump Station
City Council is requested to adopt a resolution to accept \$400,000 in grant funds from the American Rescue Plan Act (ARPA) offered by the North Carolina Department of Environmental Quality for design efforts to upgrade the Whites Mill sanitary sewer lift station.
Attachments: [Resolution - Whites Mill Pump Station - American Rescue Plan Act Grant Fundi](#)
- [2023-213](#) Contract - JWC Environmental Inc. - Eastside Wastewater Treatment Plant (WWTP)
City Council is requested to award a contract to JWC Environmental Inc. in the amount of \$253,815 for the purchase of a fine bar screen and washer compactor to replace the existing mechanical screen (#2) and compactor that is no longer functional at the Eastside Wastewater Treatment Plant (WWTP).
Attachments: [Contract - Eastside WWTP- Bar Screen Replacement](#)
- [2023-222](#) Resolution - Retire and Sale of Police K-9 Jinx

City Council is requested to adopt a resolution to retire Police K-9 Jinx and declare as surplus property to allow him to be purchased by Officer Terence Garrison who will assume all responsibility and liability for Gunner's care.

Attachments: [1. Resolution - Retire and Sale of Police K-9 Jinx](#)

[2023-223](#)

Contract - Sole Source - Forensic Technology, Inc. - BrassTrax System
City Council is requested to procure a BrassTraxHD3D Cartridge Case Acquisition Station with triage scope using the sole source bid recommendation from Forensic Technology, Inc. and authorization for the appropriate City Officials to negotiate terms and execute a contract.

Attachments: [2. Contract – Sole Source – Forensic Technology, Inc. - BrassTrax System](#)

[2023-224](#)

Contract - Long Foundation Drilling Co. - Transmission Pole Foundation
City Council is requested to award a contract to Long Foundation Drilling Company in the amount of \$322,276 to relocate a portion of 100kV transmission poles to accommodate the substation rehabilitation work at Jackson Lake Substation.

Attachments: [3. Contract – Long Foundation Drilling Co. – Transmission Pole Foundation](#)

[2023-225](#)

Budget Amendment - Agreement - SW Guilford County Fire Hydrant Agreement - High Point Fire Department
City Council is requested to approve an agreement and a budget amendment with Guilford County to fund the installation of eleven (11) Fire Hydrants in Southwest Guilford County.

Attachments: [7. Budget Amendment - Agreement – SW Guilford County Fire Hydrant Agreement](#)

[2023-226](#)

Consideration of Funding - Outside Non-Profit Organizations
City Council is requested to finalize recommendation for funding the outside organization requests.

Attachments: [8. Consideration of Funding – Outside Non-Profit Organizations](#)

[2023-227](#)

Information Regarding Resolution - SELS USA LLC Project - NC Building Reuse Grant
City Council is requested to consider a request to approve a local match for a State of North Carolina Building Reuse Grant for SELS USA LLC not to exceed \$5,000. A public hearing will be conducted at the May 15, 2023 City Council meeting.

Attachments: [9. Resolution - SELS USA LLC Project – NC Building Reuse Grant](#)

[2023-228](#)

Information Regarding Dive Bar - Performance Based Incentives
City Council is asked to consider a request from Dive Bar, to authorize performance-based incentives for a retail project at 312 N. Elm St. in the amount of \$124,798 and authorize the City Manager to execute a performance agreement with the company containing benchmarks for the company to achieve and a schedule for the payment of such financial incentives. A public hearing will be conducted at the May 15, 2023 City Council Meeting.

Attachments: [10. Dive Bar – Performance Based Incentives](#)

ADJOURNMENT



City of High Point

Municipal Office Building
211 S. Hamilton Street
High Point, NC 27260

Master

File Number: 2023-211

File ID: 2023-211

Type: Agreement

Status: To Be Introduced

Version: 1

Reference:

In Control: Finance Committee

File Created: 05/04/2023

File Name:

Final Action:

Title: Amendment No. 2 - GEL Engineering of NC - Eastside Wastewater Treatment Plant
City Council is requested to approve Amendment No. 2 in the amount of \$15,700 to modify the original supplemental agreement entered on July 20, 2022 (PO Number 109917) with GEL Engineering of NC for on-call air permitting assistance at the Eastside Wastewater Treatment Plant.

Notes:

Sponsors:

Enactment Date:

Attachments: Supplemental Agreement Amendment 2– Assistance with Air Permit Reporting Requirements and Compliance GEL Engineering of NC Inc.

Enactment Number:

Contact Name:

Hearing Date:

Drafter Name: robby.stone@highpointnc.gov

Effective Date:

Related Files:

History of Legislative File

Ver- sion:	Acting Body:	Date:	Action:	Sent To:	Due Date:	Return Date:	Result:

CITY OF HIGH POINT

AGENDA ITEM



Title: Supplemental Agreement Amendment 2– Assistance with Air Permit Reporting Requirements and Compliance GEL Engineering of NC Inc.

From: Robby Stone – Public Services Director
Derrick Boone – Public Services Asst. Director

Meeting Date: May 15, 2023

Public Hearing: N/A

Advertising Date: N/A

Advertised By: On-Call

Attachments: Attachment A – Proposal – Amendment # 2

PURPOSE: This amendment modifies the original supplemental agreement entered on July 20, 2022 (PO Number 109917) with GEL Engineering of NC for on-call air permitting assistance at the Eastside Wastewater Treatment Plant. The purpose of amendment #2 is for GEL to assist the City with the quarterly compliance emissions testing of the Sorbent Polymer Composite (SPC) Adsorber as required by the EPA approved Alternate Monitoring Plan, dated March 23, 2023.

BACKGROUND: The City of High Point operates under a Title V air emissions permit at the Eastside WWTP. The air permit includes numerous reporting requirements and annual compliance emissions testing of the fluidized bed incinerator. The recently approved Alternate Monitoring Plan by the EPA requires quarterly emissions testing of the SPC Adsorber. Amendment #2 will cover the quarterly emissions test of the (SPC) Adsorber that is scheduled in June. The other three (3) required quarterly emissions testing events will occur in the FY 2023/2024 budget year.

BUDGET IMPACT: Funds for this are available in the current budget.

RECOMMENDATION / ACTION REQUESTED: The Public Services Department recommends approval of Amendment No. 2 to GEL Engineering of NC Inc. for \$ 15,700.



Supplemental Agreement – Amendment No. 2

Date: April 27, 2023

Amendment No. 2

Project No.: HIPT00223

Project Description:

On-Call Engineering Services – Air Permitting Assistance Eastside Wastewater Treatment Plant 2022-23 Air Permit No. 08074T15 – Supplemental Agreement

To: Derrick Boone

Original Agreement Amount (Contract and/or Purchase Order):	\$69,750
Previously Authorized Change Orders:	\$10,125
This Change Order:	<u>\$15,700</u>
Revised Agreement Amount:	\$95,575

This order covers the contract modification/amendment hereunder described:

Quarterly compliance emissions testing of the SPC Adsorber (CD-04) (3 events) as required the EPA-approved (March 23, 2023) Alternate Monitoring Plan. It is assumed that the 4th event will be performed during the annual compliance emissions test in September 2023.

The work covered by this change order shall be performed under the same Terms and Conditions as included in the original Agreement.

Change Order Approved: Yes No Date: _____

Client:

By: _____

Name/Title: _____

GEL Engineering, LLC

By: Keith D McCulloch

Name/Title: Keith D. McCulloch – Director/Principal

GEL Engineering of NC, Inc.

An affiliate of the GEL Group, Inc.



City of High Point

Municipal Office Building
211 S. Hamilton Street
High Point, NC 27260

Master

File Number: 2023-212

File ID: 2023-212

Type: Resolution

Status: To Be Introduced

Version: 1

Reference:

In Control: Finance Committee

File Created: 05/04/2023

File Name:

Final Action:

Title: Resolution - American Rescue Plan Act Grant Funding (ARPA) - Whites Mill Pump Station
City Council is requested to adopt a resolution to accept \$400,000 in grant funds from the American Rescue Plan Act (ARPA) offered by the North Carolina Department of Environmental Quality for design efforts to upgrade the Whites Mill sanitary sewer lift station.

Notes:

Sponsors:

Enactment Date:

Attachments: Resolution - Whites Mill Pump Station - American Rescue Plan Act Grant Funding

Enactment Number:

Contact Name:

Hearing Date:

Drafter Name: robby.stone@highpointnc.gov

Effective Date:

Related Files:

History of Legislative File

Ver- sion:	Acting Body:	Date:	Action:	Sent To:	Due Date:	Return Date:	Result:

CITY OF HIGH POINT

AGENDA ITEM



Title: Whites Mill Pump Station – American Rescue Plan Act Grant Funding

From: Robby Stone – Public Services Director
Derrick Boone – Asst. Public Services Director

Meeting Date: May 15, 2023

Public Hearing: No

Advertising Date: N/A
Advertised By:

Attachments: Resolution

PURPOSE: Adoption of a resolution to accept \$400,000 in grant funds from the American Rescue Plan Act offered by the North Carolina Department of Environmental Quality for design efforts to upgrade the Whites Mill sanitary sewer lift station.

BACKGROUND: The Whites Mill lift station is a duplex sanitary sewer lift station that was upgraded circa 2006. The lift station service area consists primarily of residential properties as well as three schools. The lift station is nearing its operating capacity. The Whites Mill lift station was evaluated in November 2021. The scope of the project will consist of the design of improvements to expand the capacity of the lift station, as well as the following:

- Extension of a 10-inch diameter force main along Oak Hollow Drive and La Salle Drive to discharge immediately upstream of the La Salle Siphon
- Upsizing of 320 feet of gravity sewer and installation of a grinder in the vicinity of the La Salle Drive Siphon
- Installation of a third 8-inch siphon pipe will be installed by horizontal directional drill (HDD) across the lake to connect to the Lake Forest lift station.

The preliminary cost estimate to construct the Whites Mill Lift Station Upgrade and additional downstream sanitary sewer improvements is approximately \$5 million dollars.

BUDGET IMPACT: The NC Department of Environmental Quality issued a funding award in the total amount of \$400,000 toward the design of this project.

RECOMMENDATION / ACTION REQUESTED: Approve the attached resolution accepting the \$400,000 grant offer.

CITY OF HIGH POINT

RESOLUTION BY GOVERNING BODY OF RECIPIENT

WHEREAS, the American Rescue Plan Act (ARPA), funded from the State Fiscal Recovery Fund, was established in Session Law (S.L.) 2021-180 and S.L. 2022-74 to assist eligible units of local government with meeting their drinking water and/or wastewater and/or stormwater infrastructure needs, and

WHEREAS, the North Carolina Department of Environmental Quality has offered ARPA funding in the amount of \$400,000 to perform the work detailed in the submitted application, and

WHEREAS, the City of High Point intends to perform said project in accordance with the agreed scope of work,

NOW, THEREFORE, BE IT RESOLVED BY THE HIGH POINT CITY COUNCIL OF THE CITY OF HIGH POINT:

That the City of High Point does hereby accept the ARPA grant offer of \$400,000; and

That the City of High Point does hereby give assurance to the North Carolina Department of Environmental Quality that any *Conditions* or *Assurances* contained in the *Funding Offer and Acceptance* (award offer) will be adhered to; has substantially complied, or will substantially comply, with all federal, State of North Carolina (State), and local laws, rules, regulations, and ordinances applicable to the project; and to federal and State grants and loans pertaining thereto; and

That City Manager, and successors so titled, is hereby authorized and directed to furnish such information as the appropriate State agency may request in connection with this project; to make the assurances as contained above; and to execute such other documents as may be required by the North Carolina Department of Environmental Quality, Division of Water Infrastructure.

Adopted by High Point City Council this May 15, 2023 in High Point, North Carolina.

[SEAL]

Jay W. Wagner, Mayor

Sandra Keeney, City Clerk

CERTIFICATION BY RECORDING OFFICER

The undersigned duly qualified and acting [title of officer] of the City of High Point does hereby certify: That the above/attached resolution is a true and correct copy of the resolution authorizing the filing of an application with the State of North Carolina, as regularly adopted at a legally convened meeting of the High Point City Council duly held on the 15th day of May, 2023; and, further, that such resolution has been fully recorded in the journal of proceedings and records in my office. IN WITNESS WHEREOF, I have hereunto set my hand this _____ day of _____, 2023.

(Signature of Recording Officer)

(Title of Recording Officer)



City of High Point

Municipal Office Building
211 S. Hamilton Street
High Point, NC 27260

Master

File Number: 2023-213

File ID: 2023-213

Type: Miscellaneous Item

Status: To Be Introduced

Version: 1

Reference:

In Control: Finance Committee

File Created: 05/04/2023

File Name:

Final Action:

Title: Contract - JWC Environmental Inc. - Eastside Wastewater Treatment Plant (WWTP)
City Council is requested to award a contract to JWC Environmental Inc. in the amount of \$253,815 for the purchase of a fine bar screen and washer compactor to replace the existing mechanical screen (#2) and compactor that is no longer functional at the Eastside Wastewater Treatment Plant (WWTP).

Notes:

Sponsors:

Enactment Date:

Attachments: Contract - Eastside WWTP- Bar Screen Replacement

Enactment Number:

Contact Name:

Hearing Date:

Drafter Name: robby.stone@highpointnc.gov

Effective Date:

Related Files:

History of Legislative File

Ver- sion:	Acting Body:	Date:	Action:	Sent To:	Due Date:	Return Date:	Result:

CITY OF HIGH POINT AGENDA ITEM



Title: Contract - JWC Environmental Inc. Eastside Waste Water Treatment Plant

From: Robby Stone – Public Services Director
Derrick Boone – Asst. Director Public Services

Meeting Date: May 15, 2023

Public Hearing: No

Advertising Date: N/A
Advertised By: N/A

Attachments: Attachment A – Bid Tabulation
Attachment B- Additional Equipment Information

PURPOSE:

To purchase a fine bar screen and washer compactor that will replace the existing mechanical screen (#2) and compactor that is no longer functional at the Eastside Wastewater Treatment Plant (WWTP).

BACKGROUND:

The Eastside WWTP has three mechanical bar screens at the plant influent that function as part of the preliminary treatment process. A bar screen is a mechanical filter used to remove large objects, such as rags and plastics, from wastewater (see picture below). The mechanical bar screen in the #2 location is 20-years old, and it has been difficult to obtain replacement parts and technical support from the manufacturer. The Public Services Department received two bids for a replacement bar screen. The lowest bidder is JWC Environmental Inc. with a base bid of \$213,935 for a fine screen unit /washer compactor and an alternate bid of \$39,880 for a dual shafted grinder.

BUDGET IMPACT:

Funds for this project are available in the FY 2022-2023 budget.

RECOMMENDATION / ACTION REQUESTED:

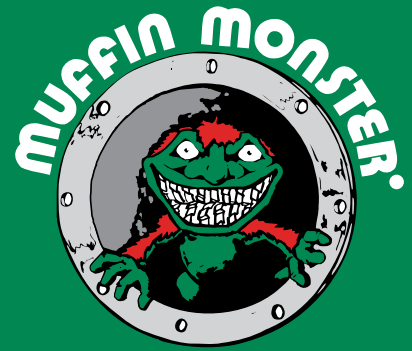
The Public Services Department recommends awarding the contract to JWC Environmental Inc. in the total amount of \$253,815 which includes the alternate bid item.



Example Bar Screen at the Eastside WWTP

**Bid Tabulation
City of High Point, North Carolina
Fine Bar Screen and Compactor Replacement
Bid 37-050323**

Contractor	Fine Screening Unit	Washer, Compactor	Total Base Bid Price	Alternate Bid (Dual Shafted Grinder)
Parkson Corp	\$229,000.00	Included	\$229,000	N/A
JWC Environmental	\$169,450.00	\$44,485.00	\$213,935.00	\$39,880.00



Monster Separation Systems®

FINESCREEN MONSTER®



The Finescreen Monster provides a high capture rate of wastewater solids, including small debris. It incorporates a continuous band of stainless steel panels or optional StapleGuard ultra high molecular weight (UHMW) polyethylene perforated panels attached to heavy-duty stainless steel roller chains. Panels are available with 1/8" or 1/4" (3 or 6 mm) openings. Stainless steel rollers track in UHMW guides at the bottom of the screen, thus eliminating the need for sprockets or bearings submerged in the wastewater flow.

Advanced Design

- Completely stainless steel.
- UHMW side seals and Buna-N rubber with polypropylene bristle bottom sealing strip prevent debris from passing around the screen.

Enhanced Cleaning System

- Brushless cleaning system using water spray with UHMW panels.
- Lower maintenance and better panel cleaning.

Ease of Maintenance

- Easy to lift access covers and easy to reach assembly allows simple fine tuning.

Staple Guard UHMW Polyethylene Perforated Panels (optional)

- Reduces stapling (or hair pinning) on the panels.
- Highly abrasion, wear and corrosion resistant.

Equipment Sizing

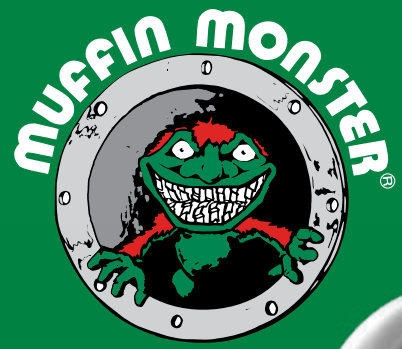
Screen Panel Hole Size: \varnothing 1/8" or 1/4" (3 or 6 mm) holes

Depth: Up to 40' (12.2 m) with a max 6' (1.8 m) discharge height

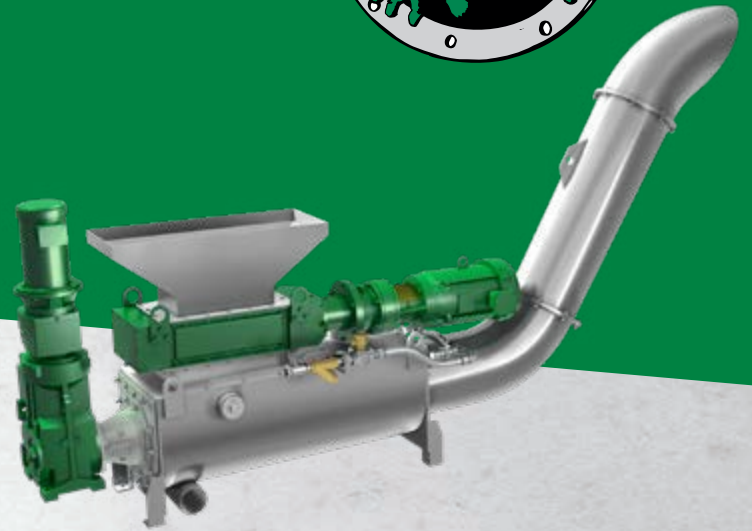
Width: 2' to 8' (.6 to 2.4 m)

Angle: 60° to 85° inclination; 70° standard





MONSTER WASH PRESS



The Monster Wash Press is JWC Environmental's latest generation of washer compactors. The Monster Wash Press processes screenings to separate water and organics from the solids. The result is a clean, dry, light and compact discharge which reduces the amount of waste to be dumped, ultimately saving treatment facilities time and money.

The Monster Wash Press may be outfitted with a Muffin Monster® grinder to pre-condition the screenings before they enter the washer compactor. The grinder breaks open rags, plastics and trash to promote washing and removal of soft organics during the wash cycle. Additionally, pre-conditioned screenings result in superior compaction, reducing the volume of discharge that must be hauled away.

Discharge from the pre-conditioning Muffin Monster or directly from the screen enters a Pre-Wash Zone where the debris is soaked to begin the process of separating organics from the solids. An auger rotor transports the soaked debris into the Active Wash Zone of the Monster Wash Press where a paddle rotor* agitates the material, enhancing wash water penetration throughout the debris. The soft organic washed from the solids pass through a screen and return to the plant's waste stream for treatment. The washed solids are moved to the Transport and Compaction Zone where water is removed and the solids are compacted. The resultant discharge emerges from the Monster Wash Press as a dry, solid plug.

Features and Benefits

Dual Shafted Grinder (optional)

- 30K Muffin Monster grinds screenings discharge for the best washing and compacting
- Easy to retrofit grinderless Monster Wash Press with Muffin Monster

Pre-Wash Zone

- Soaks screenings to jump-start separation of organics from solids
- Brushless auger rotor to promote free movement of debris to active wash zone

Active Wash Zone

- Paddle rotor* mixes and break-ups debris in wash zone to optimize separation of soft organics from solids
- Brushed rotor keeps screen clean
- 2, 3, or 6 mm perforated screens to separate solids from organics

Easy Maintenance

- Segmented auger rotor brush for easy brush replacement
- Removable top cover and drive end plate* minimizes clearance space needed to remove rotor and screen
- Field replaceable screen
- Multiple inspection ports for easy examination of equipment and operation

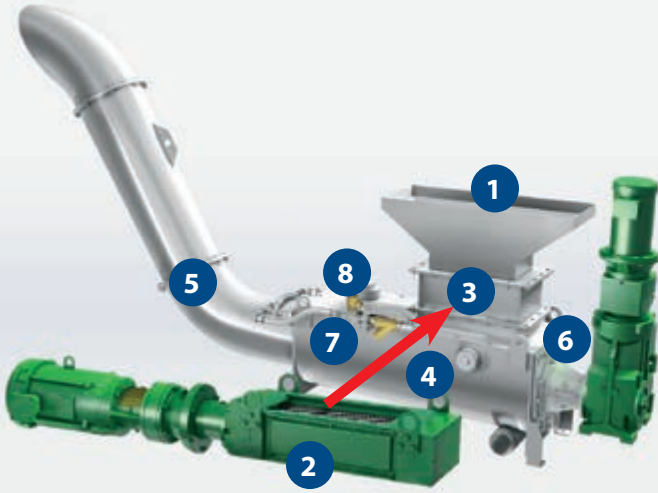


The Monster Wash Press is available only in North America

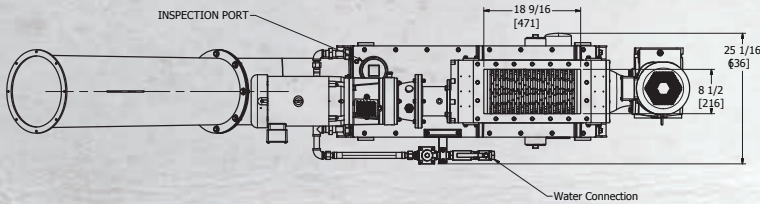
* Patent Pending

www.jwce.com

Monster wash press details



1. Hopper collect screenings
2. Muffin Monster grinds up material (optional)
3. Easy to install grinder later
4. Active Wash Zone cleans screenings
5. Cleaned discharge is dewatered and compacted
6. Removable top cover and drive end plate for easy removal of rotor and screen
7. Segmented rotor brush for easy brush replacement
8. Inspection ports

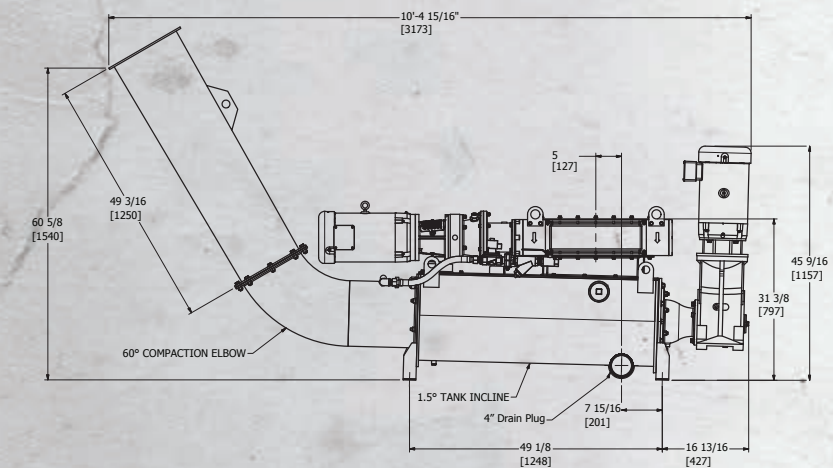
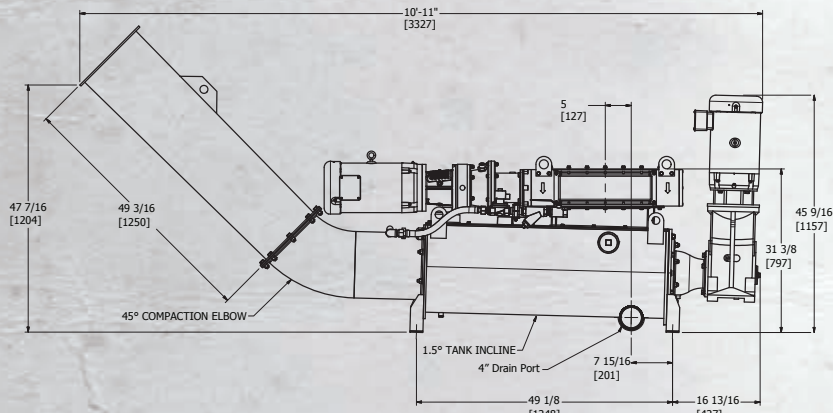


Standard Construction

- Tank, screen, compaction elbow and transport tube: 304 stainless steel
- Auger rotor: Alloy steel
- Grinder with MWP3018: Ductile iron housing, hardened alloy steel cutters

Optional Equipment

- 316 stainless steel tank, screen, compaction elbow and transport tube
- Discharge bagger
- Stainless steel roller base
- Discharge tip
- Customized hopper
- Customized discharge transport assembly



STANDARD FEATURES

	MWP0018	MWP3018
Grinder Motor - hp (kW)	N/A	10 (7.5)
Auger Screw Motor - hp (kW)	5 (3.7)	5 (3.7)
Upgradeable to Add Grinder	Yes	Grinder Included
Dry Weight w/Controller - lb (kg)	1425 (647)	2025 (920)

PERFORMANCE

	MWP0018	MWP3018
Continuous Throughput - ft ³ /hr (m ³ /hr)	206 (5.8)	78 (2.2)
Batch Output - ft ³ /hr (m ³ /hr)	120 (3.4)	46 (1.3)
Water Capacity* - gpm (l/s)	280 (17.7)	

*For 3mm or 6mm perforated screen

The Monster Wash Press is available only in North America



Headquarters
 2850 Red Hill Ave., Suite 125
 Santa Ana, CA 92705 USA
 toll free: 800.331.2277
 phone: 949.833.3888
 fax: 949.833.8858
 email: jwce@jwce.com

www.jwce.com





FORMAL BID RECOMMENDATION
REQUEST FOR COUNCIL APPROVAL

DEPARTMENT: Public Services Department

COUNCIL AGENDA DATE: May 15, 2023

BID NO.: 37-050323 CONTRACT NO.: DATE OPENED: May 3, 2023

DESCRIPTION:

Fine Bar Screen and Compactor

PURPOSE:

To purchase a fine bar screen and washer compactor that will replace the existing mechanical screen (#2) and compactor that is no longer functional at the Eastside Wastewater Treatment Plant (WWTP).

COMMENTS:

RECOMMEND AWARD TO: JWC Environmental Inc. AMOUNT: \$253,815.00

JUSTIFICATION:

Lowest Bidder

ACCOUNTING UNIT	ACCOUNT	ACTIVITY	CATEGORY	BUDGETED AMOUNT
621757	533101			\$253,814.00
TOTAL BUDGETED AMOUNT				

DEPARTMENT HEAD: Robby Stone Digitally signed by Robby Stone Date: 2023.05.04 07:50:03 -04'00' DATE: 5-4-2023

The Purchasing Division concurs with recommendation submitted by the and recommends award to the lowest responsible, responsive bidder in the amount of \$.

PURCHASING MANAGER: Candy E. Harmon Digitally signed by Candy E. Harmon Date: 2023.05.04 08:05:04 -04'00' DATE: 5-4-2023

Approved for Submission to Council
FINANCIAL SERVICES DIRECTOR: Bobby Fitzjohn Digitally signed by Bobby Fitzjohn Date: 2023.05.04 08:11:45 -04'00' DATE: 5-4-2023

CITY MANAGER: DATE:



City of High Point

Municipal Office Building
211 S. Hamilton Street
High Point, NC 27260

Master

File Number: 2023-222

File ID: 2023-222

Type: Resolution

Status: To Be Introduced

Version: 1

Reference:

In Control: City Council

File Created: 05/08/2023

File Name:

Final Action:

Title: Resolution - Retire and Sale of Police K-9 Jinx
City Council is requested to adopt a resolution to retire Police K-9 Jinx and declare as surplus property to allow him to be purchased by Officer Terence Garrison who will assume all responsibility and liability for Gunner's care.

Notes:

Sponsors:

Enactment Date:

Attachments: 1. Resolution - Retire and Sale of Police K-9 Jinx

Enactment Number:

Contact Name:

Hearing Date:

Drafter Name: amy.myers@highpointnc.gov

Effective Date:

Related Files:

History of Legislative File

Ver- sion:	Acting Body:	Date:	Action:	Sent To:	Due Date:	Return Date:	Result:

CITY OF HIGH POINT AGENDA ITEM



Title: Request to Retire and Sell K-9 Jinx

From: J. Travis Stroud, Chief of Police

Public Hearing: N/A

Attachments: Photo
Resolution

Meeting Date: May 15, 2023

**Advertising Date /
Advertised By:** N/A

PURPOSE:

The Police Department is requesting consideration for approval to retire (declare surplus) Police K-9 Jinx.

BACKGROUND:

The High Point Police Department purchased Canine Jinx from Houston K-9 Academy of Houston, TX, in July 2019 for \$10,000.00. Jinx was purchased to maintain the appropriate level of the K-9 Unit's working animals. K-9 Jinx served as a dual-purpose patrol canine from July 2019 until April 2023. At his age, it would be difficult to transfer him to a new handler to continue his work life and the Department wishes to retire him.

BUDGET IMPACT:

Officer Terence Garrison has agreed to purchase retired K-9 Jinx from the City of High Point in the amount of \$1.00 and upon accepting custody of the dog will assume all liability and responsibility for the care of the animal for the remainder of its life.

Due to Jinx's pending retirement, the Department has purchased a replacement K-9 for \$13,500 in FY 23 with General Budget Funds identified within the Support Services Division's budget.

RECOMMENDATION / ACTION REQUESTED:

The Police Department requests that K-9 Jinx be declared surplus property and for City Council to authorize the purchase of K-9 Jinx by Officer Terence Garrison.



RESOLUTION AUTHORIZING THE SALE OF
RETIRED K-9 JINX

WHEREAS, the City Council for the City of High Point finds that Police K-9 Jinx can no longer perform as required for his job and has received a recommendation from the High Point Police Department K-9 Supervisor that Jinx be retired; and

WHEREAS, N.C.G.S. 160A-266(d) permits the City Council to authorize the disposition of personal property that is without value; and

WHEREAS, Officer Terence Garrison has agreed to purchase retired K-9 Jinx from the City of High Point in the amount of \$1.00 and upon accepting custody of the dog will assume all liability and responsibility for the care of the animal for the remainder of its life.

NOW, THEREFORE, BE IT RESOLVED, that the City Council of the City of High Point authorizes the purchase of K-9 Jinx by Officer Terence Garrison for \$1.00 effective May 15, 2023.

Adopted: _____

Jay Wagner, Mayor

ATTEST

Sandra Keeney
City Clerk



City of High Point

Municipal Office Building
211 S. Hamilton Street
High Point, NC 27260

Master

File Number: 2023-223

File ID: 2023-223

Type: Contract

Status: To Be Introduced

Version: 1

Reference:

In Control: City Council

File Created: 05/08/2023

File Name:

Final Action:

Title: Contract - Sole Source - Forensic Technology, Inc. - BrassTrax System
City Council is requested to procure a BrassTraxHD3D Cartridge Case Acquisition Station with triage scope using the sole source bid recommendation from Forensic Technology, Inc. and authorization for the appropriate City Officials to negotiate terms and execute a contract.

Notes:

Sponsors:

Enactment Date:

Attachments: 2. Contract – Sole Source – Forensic Technology, Inc. - BrassTrax System

Enactment Number:

Contact Name:

Hearing Date:

Drafter Name: amy.myers@highpointnc.gov

Effective Date:

Related Files:

History of Legislative File

Ver- sion:	Acting Body:	Date:	Action:	Sent To:	Due Date:	Return Date:	Result:
---------------	--------------	-------	---------	----------	-----------	-----------------	---------

CITY OF HIGH POINT AGENDA ITEM



Title: Ultra Forensic Technology BrassTrax System- Sole Source Purchase

From: J. Travis Stroud, Chief of Police

Meeting Date: May 15, 2023

Public Hearing: N/A

**Advertising Date /
Advertised By:** N/A

Attachments: Image
Gun-Related Crime Stats
Quote (Option 2.2 noted on page 4 of 17)
Sole Source Letter

PURPOSE:

The City Council is asked to award procurement via Sole Source to Forensic Technology, Inc. for a BrassTrax System.

BACKGROUND:

The High Point Police Department is seeking to adopt technology in the form of new-and-improved tools to aid officers in solving violent gun crimes. Access to this System will also be extended to neighboring law enforcement agencies.

Since 2019, the City of High Point has experienced increased violent firearms-related crime. In 2018 and 2019, the Department was consistently one of the top agencies submitting a high volume of shell casings to the North Carolina State Crime Lab (NCSCCL) for entry into the National Integrated Ballistic Information Network (NIBIN). NIBIN links crimes quickly, generate investigative leads that would otherwise not have been detected, shares intelligence across jurisdictional boundaries, and gives prosecutors admissible evidence to corroborate witness testimony. NIBIN is the only national network that allows for the capture and comparison of ballistic evidence to aid in solving and preventing violent crimes involving firearms. However, turnaround times for the State's dispensation of evidence are extensive (weeks to months). Having the equipment directly accessible will eliminate wait times.

The Department will use the apportioned funds of the 2019 Justice Assistance Grant (JAG) Award to procure a BrassTraxHD3D Cartridge Case Acquisition Station with a triage scope. The station captures highly detailed images of fired cartridge cases, including firing pin impressions on the primer, breech face, extractor, and injector markings. A warranty for the system's 2nd year of useful life and additional training for two staff members will also be obtained to support the System.

Forensic Technology, Inc. of Largo, Florida, is the sole source vendor of BrassTrax System and the leading provider for Law Enforcement agencies in partnership with the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF).

BUDGET IMPACT:

Funds have been identified from the 2019 JAG Federal Award of \$120,030 and General Budget Funds of \$5,017, totaling \$125,047. Funds will be requested during the FY 2024-25 budget process to sustain the annual reoccurring fees, approximated at \$50,000.

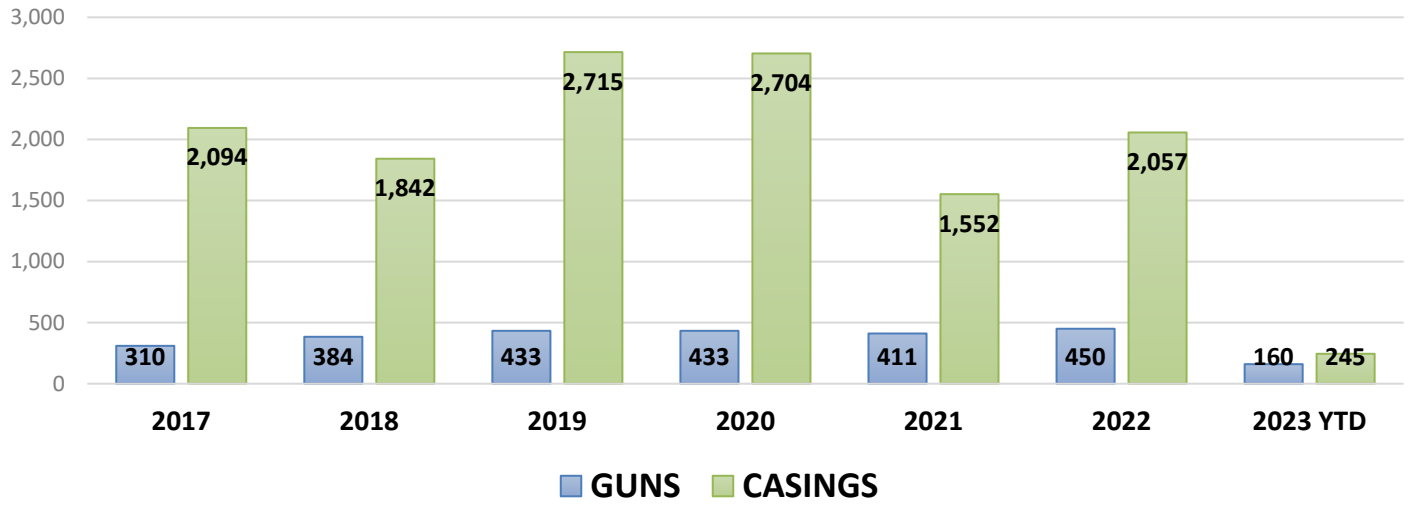
RECOMMENDATION /ACTION REQUESTED:

The Police Department requests Council approval to procure a BrassTraxHD3D Cartridge Case Acquisition Station with triage scope using the sole source bid recommendation from Forensic Technology, Inc. and authorization for the appropriate City Officials to negotiate terms and execute a contract.



**HIGH POINT POLICE DEPT
GUNS & CASINGS BY YEAR: 2017-2023 YTD**

2017-2022 % CHG: GUNS +45% / CASINGS -2%



Financial Services

Purchasing Division



NORTH CAROLINA'S INTERNATIONAL CITY™

Requisition # []

CITY OF HIGH POINT
SOLE SOURCE JUSTIFICATION FORM
(For Items Costing \$10,000.00 or More)
Statutory Reference N.C.G.S. 143-129(e)6

Vendor: Forensic Technology, Inc.

Item(s): BrassTrax System

Justification:

Only Forensic Technology, the exclusive manufacturer of IBIS and Quantum 3D Microscope (Q3M), can provide their proprietary products IBIS BRASSTRAX, IBIS BULLETTRAX, IBIS MATCHPOINT, IBIS Data Concentrator, IBIS Correlation Engine, and Q3M, as well as maintenance, upgrades and services, including data migration, moving and training services thereto.

Estimated expenditure for the above item(s): 125,047

Accounting Unit and Account(s): 301310 533101 301191060205 55310 &101312

CHECK ALL ENTRIES BELOW THAT APPLY TO THE PROPOSED PURCHASE. ATTACH A MEMO CONTAINING JUSTIFICATION AND SUPPORT DOCUMENTATION.

- 1. [] Performance or price competition for a product are not available.
2. [x] A needed product is available from only one source of supply.
3. [] Standardization or compatibility is the overriding consideration.
4. [] The parts/equipment are required from this source to permit standardization.
5. [] None of the above applies. A detailed explanation and justification for this sole source request is contained in attached memo and support documentation.

The undersigned requests that competitive procurement be waived and that the vendor identified as the supplier of the material or service described in this sole source justification be authorized as a sole source for the material or service.

Department Head/Authorized Personnel J. Travis Stroud Digitally signed by J. Travis Stroud Date: 2023.05.08 08:27:37 -04'00'

Department/Division Police Date []

APPROVAL PROCESS

Purchasing Manager []

Financial Services Director []

City Council (\$30,000 - Up) []

ULTRA

February 15, 2023

High Point Police Department
1730 Westchester Drive
High Point, North Carolina, 27262
United States

Ultra Electronics Forensic Technology Inc.

800 Hymus Blvd, 4th floor
St-Laurent, Quebec
H4S 0B5
Canada

Tel +1 514 489 4247
Fax +1 514 485 9336
Sans Frais/TollFree +1 888 984 4247
www.ultra-forensictechnology.com

Subject: Sole Source Letter

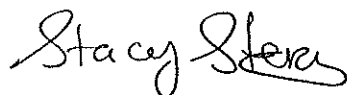
To whom it may concern:

The Integrated Ballistic Identification System (IBIS®) uses technology that encompasses several patents protected in the United States and throughout the world. As such, manufacturing and servicing these products require access to proprietary and commercially sensitive information that is only accessible to employees of **Ultra Electronics Forensic Technology Inc.** and its affiliate company **Forensic Technology Inc.** (hereinafter collectively referred to as **Forensic Technology**).

Consequently, only Forensic Technology, the exclusive manufacturer of IBIS and Quantum 3D Microscope™ (Q3M), can provide their proprietary products IBIS BRASSTRAX, IBIS BULLETRAX, IBIS MATCHPOINT, IBIS Data Concentrator, IBIS Correlation Engine, and Q3M, as well as maintenance, upgrades and services, including data migration, moving and training services pertaining thereto.

Furthermore, IBIS, currently in use in the United States under the ATF NIBIN program, is the only technology that has undergone extensive testing and complies with the security standards needed for integration into NIBIN. Other ballistic identification technologies are not compatible with NIBIN.

Sincerely yours,



Stacy Stern
Vice President Sales and Marketing

ABOUT ULTRA ELECTRONICS FORENSIC TECHNOLOGY



Forensic Technology is a leading provider of forensic investigation and analysis tools used by law enforcement agencies around the world to keep their societies safe.

We created **IBIS**® (the Integrated Ballistic Identification System) in 1991 and are pioneers in automated ballistics identification. IBIS helps forensic experts provide detectives with timely information about guns, crimes, and suspects. It does so by suggesting possible matches between pairs of fired bullets and cartridge cases. It finds the proverbial "needle in the haystack" and it does so at speeds well beyond human capabilities. In 2011 we added forensic document examination to our portfolio of solutions through our purchase of Swiss-based Projectina AG, a manufacturer of optical and opto-electronic systems.

Forensic Technology is a customer-driven organization that partners with hundreds of public safety agencies in over 130 countries. We provide cost-effective crime-fighting solutions a solid corporate infrastructure that governments can call upon for forensic investigation and analysis.

With vast experience in scalable, sustainable, networked solutions, our engineering, forensic, and law-enforcement professionals provide worldwide 24/7-customer support and dedicated training facilities. Our products are powerful tools that can be used for independent examination. But when networked, they become powerful systems that facilitate data analysis and intelligence sharing among agencies and across jurisdictional boundaries.

In 2014, we joined Ultra Electronics, a successful international defense, security, transport, and energy company. Ultra has a long and consistent record of innovating and engineering solutions that satisfy customer requirements (www.ultra-electronics.com).

Forensic Technology helps law-enforcement agencies around the world achieve higher levels of performance in the fight against crime. We continue to innovate so the world can be a safer place.

For more information, please visit www.ultra-forensictechnology.com.

ULTRA

Follow us    
www.ultra-forensictechnology.com

DOJ 2640.2F



INFORMATION TECHNOLOGY SECURITY

Approval Date: November 26, 2008

Approved By: LEE J. LOFTHUS
Assistant Attorney General for Administration

Distribution: BUR/H-1; OBD/H-1; SPL-23

Initiated By: Department Chief Information Officer

FOREWORD

1. **PURPOSE.** This order establishes uniform policy, responsibilities and authorities for protection of Information Technology (IT) systems that store, process or transmit Department of Justice (Department) information.
2. **SCOPE.** The provisions of this order apply to all Department Components, personnel and IT systems used to process, store or transmit Department information. They apply to contractors and other users of IT systems supporting the operations and assets of the Department, including any non-Department organizations and their representatives who are granted access to Department IT resources, such as other Federal agencies. This policy applies to IT systems processing National Security Information and unclassified information.
3. **CANCELLATION.** Department Order 2640.2E is cancelled.
4. **AUTHORITIES.** The Department Chief Information Officer (CIO) is responsible for providing policy, guidance, implementation and oversight for IT systems.
5. **REPERCUSSIONS FOR COMPONENT NON-COMPLIANCE.** The Department CIO may take appropriate action if a Component, contractor or other non-Department organization or their representatives are found to be non-compliant with Department IT security policy. The Department Chief Information Security Officer (CISO), and Department Security Officer (DSO) shall be notified in cases of such non-compliance in order to take appropriate action.

6. **REFERENCES.** References to various regulations and laws applicable to the responsibilities of IT security are located in APPENDIX 1. Future updates to referenced documents will be considered applicable to this order.

7. **DEFINITION OF TERMS.** Terms shall have the meaning defined by National Institute of Standards and Technology Interagency Reports (NISTIRs), Federal Information Processing Standards (FIPS) and Special Publications (SP). Unless otherwise stated, all terms used in NIST publications are also consistent with the definitions contained in the Committee on National Security Systems Instruction No. 4009, National Information Assurance Glossary.

/s/LEE J. LOFTHUS
Assistant Attorney General
for Administration

TABLE OF CONTENTS

TABLE OF CONTENTS	3
1. Component Information Technology Security Programs	5
2. Required Use of DOJ IT Systems	5
3. Management Security Policy	5
4. Operational Security Policy	6
5. Technical Security Policy	9
6. National Security Systems and Sensitive Compartmented Information (SCI) IT Systems	11
7. Classified Laptop and Mobile Computing Devices	11
8. Use of DOJ IT Resources Outside US Territory.	11
9. Facsimile	12
CHAPTER 2. ISSUE-SPECIFIC SECURITY POLICIES.....	12
10. Sensitive and Personally Identifiable Information (PII)	12
11. External Information Systems.....	13
12. Protection of Mobile Computers/Devices and Removable Media	14
13. Remote Access to DOJ Systems	14
14. Contractors	15
CHAPTER 3. DETERMINING SECURITY CONTROL REQUIREMENTS.....	16
15. Applicability	16
16. Categorize information types and information systems.....	16
17. Select, tailor and supplement initial baseline security controls	17
18. Implement security controls.....	17
19. Assess and Authorize the implemented controls	17
20. Monitor	18
CHAPTER 4. ROLES AND RESPONSIBILITIES	18
21. Department Chief Information Officer	18
22. Chief Information Security Officer.....	20
23. Department Security Officer.....	21
24. Component Heads or Their Designee(s).....	22

CHAPTER 5. AGENCY-WIDE PROGRAM IMPLEMENTATION..... 23

 25. Core Program 23

 26. IT Security Management Strategy 24

APPENDIX 1. REFERENCES..... 27

 1. Congressional Mandates 27

 2. Federal/Departmental Regulations/Guidance 27

 3. Presidential and Office of Management and Budget Guidance..... 30

CHAPTER 1. INFORMATION TECHNOLOGY SECURITY POLICY

1. Component Information Technology Security Programs.

Each Component shall establish and maintain an IT security program, in compliance with the Department's overall IT security program, to ensure the confidentiality, integrity and availability of the Component's computer systems, networks and data, in accordance with all Federal and Department policies, standards, procedures and guidance.

2. Required Use of DOJ IT Systems

DOJ information used for official business may only be processed, stored, or transmitted on IT systems meeting the requirements of this order.

This restriction does not apply to DOJ information disseminated to other Federal, State, Local or Tribal agencies, or to information released to the public or as part of a court proceeding, or to information whose release is required to accomplish a non-DOJ function (e.g., information released to a hospital so it can provide health care services to a prisoner).

3. Management Security Policy

- a. **Risk Assessment.** In accordance with DOJ IT Security Standard - Risk Assessment (RA) Control Family, Components shall periodically assess the risk to Departmental operations (including mission, function, image or reputation) and assets, individuals, other organizations, and the Nation resulting from the operation of Department IT systems and the associated processing, storage, or transmission of Department information.
- b. **Planning.** In accordance with DOJ IT Security Standard – Planning (PL) Control Family, Components shall develop, document, periodically update and implement security plans for Department IT systems that describe the security controls in place or planned for the IT systems and the rules of behavior for individuals accessing the IT systems.
- c. **System and Services Acquisition.** In accordance with DOJ IT Security Standard – System and Services Acquisition (SA) Control Family, Components shall:
 - (1) Allocate sufficient resources to adequately protect Department IT systems.
 - (2) Employ systems development life cycle processes that incorporate IT security considerations.
 - (3) Ensure new acquisitions include available Commonly Accepted Security Configurations.

- (4) Perform acquisition risk assessments, and develop and adopt effective supply chain risk mitigation for IT acquisitions.
- (5) Employ software usage and installation restrictions to ensure software installed on Component IT systems is in compliance with applicable copyright laws and licensing agreements.
- (6) Ensure third-party providers are contractually required to comply with this policy to employ adequate security measures to protect information, applications and/or services outsourced from the Department.

d. **Certification, Accreditation and Security Assessments.** In accordance with DOJ IT Security Standard – Certification, Accreditation and Security Assessments (CA) Control Family, Components shall:

- (1) Periodically assess the security controls in Component IT systems to determine if the controls are effective in their application.
- (2) Develop, monitor and implement plans of action and milestones (POA&M) designed to correct deficiencies and reduce or eliminate vulnerabilities in Component IT systems.
- (3) Authorize the operation of Component IT systems and any associated IT system interconnections prior to operational use, and notify the Component CIO.
- (4) Monitor IT system security controls on an ongoing basis to ensure the continued effectiveness of the controls.

4. Operational Security Policy

a. **Personnel Security.** In accordance with DOJ IT Security Standard – Personnel Security (PS) Control Family, Components shall:

- (1) Ensure individuals occupying positions of responsibility within the Component (including third-party service providers) are trustworthy and meet established security criteria for those positions.
- (2) Ensure Non-United States (U.S.) citizens are not authorized to access or assist in the development, operation, management or maintenance of Component IT systems, unless a waiver has been granted by the Component Head, with the concurrence of the Department Chief Information Officer (CIO) and Department Security Officer (DSO).
- (3) Ensure Component information and IT systems are protected during and after personnel actions such as terminations and transfers.

- (4) Employ formal sanctions for personnel failing to comply with Department security policy and procedures.
- b. **Physical and Environmental Protection.** In accordance with DOJ IT Security Standard – Physical and Environmental Protection (PE) Control Family, Components shall:
- (1) Limit physical access to IT systems, equipment and the respective operating environments to authorized individuals and monitor and log all such accesses.
 - (2) Protect the physical plant and support infrastructure for IT systems.
 - (3) Provide supporting utilities for IT systems.
 - (4) Protect IT systems against environmental hazards.
 - (5) Provide appropriate environmental controls in facilities containing information systems.
- c. **Contingency Planning.** In accordance with DOJ IT Security Standard – Contingency Planning (CP) Control Family, Components shall establish, maintain and effectively implement plans for emergency response, backup operations and post-disaster recovery for Component IT systems to ensure the availability of critical IT resources and continuity of operations in emergency situations.
- d. **Configuration Management.** In accordance with DOJ IT Security Standard – Configuration Management (CM) Control Family, Components shall:
- (1) Establish and maintain baseline configurations and inventories of Component IT systems (including hardware, software, firmware and documentation) throughout the respective system development life cycle.
 - (2) Establish a configuration change control process to ensure proposed changes are evaluated, tested, properly approved and documented before being put into production.
 - (3) Establish and enforce security settings consistent with the information system operational requirements and Department commonly accepted security configurations (e.g., Federal Desktop Core Configuration) and validate those controls through Department approved tools.
- e. **Maintenance.** In accordance with DOJ IT Security Standard – Maintenance (MA) Control Family, Components shall:
- (1) Perform periodic and timely maintenance on Component IT systems.

- (2) Provide effective controls on the tools, techniques, mechanisms and personnel used to conduct on-site and remote IT system maintenance.
- f. **System and Information Integrity.** In accordance with DOJ IT Security Standard – System and Information Integrity (SI) Control Family, Components shall:
- (1) Identify, report and correct information and information system flaws in a timely manner.
 - (2) Provide protection from malicious code at appropriate locations within Component IT systems.
 - (3) Monitor IT system security alerts and advisories and take appropriate actions in response.
- g. **Media Protection.** In accordance with DOJ IT Security Standard – Media Protection (MP) Control Family, Components shall:
- (1) Protect IT system media, both paper and digital.
 - (2) Encrypt sensitive and classified information transported outside of the agency’s secured, physical perimeter in digital format (including information transported on removable media such as USB drives, CDs, DVDs and on portable/mobile devices such as laptop computers and/or personal digital assistants) using FIPS 140-2 validated or NSA approved encryption, as appropriate.
 - (3) Limit access to information on IT system media to authorized users.
 - (4) Sanitize or destroy IT system media before disposal or release for reuse.
 - (5) Stipulate in contracts for equipment maintenance warranty that equipment to be removed from the Component’s physically protected offices shall be sanitized before removal.
- h. **Incident Response.** In accordance with DOJ IT Security Standard – Incident Response (IR) Control Family, Components shall:
- (1) Establish an operational incident handling capability for Component IT systems that includes adequate preparation, detection, analysis, containment, recovery and user response activities in coordination with the Department of Justice Computer Emergency Response Team (DOJCERT).
 - (2) Track, document and report incidents to appropriate Department officials and/or authorities.

- (3) Provide Department forensics and law enforcement personnel access to media and devices required for investigation, when appropriate.
 - (4) Assist with digital forensics on electronic devices and/or associated media.
 - (5) Maintain a chain of custody to record the handling and transfer of media and devices to support investigations and forensics.
- i. **Awareness and Training.** In accordance with DOJ IT Security Standard – Awareness and Training (AT) Control Family, Components shall:
- (1) Ensure managers and users of Component and Department IT systems are aware of the security risks associated with their activities and of the applicable laws, Executive Orders, directives, policy, standards, instructions, regulations, or procedures related to the security of Component and Department IT systems and data, including digital and paper.
 - (2) Ensure Component personnel are adequately trained to carry out their assigned IT security-related duties and responsibilities.

5. Technical Security Policy

- a. **Identification and Authentication.** In accordance with DOJ IT Security Standard – Identification and Authentication (IA) Control Family, Component IT systems shall:
- (1) Identify IT system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to Component IT systems.
 - (2) Allow remote access only with two-factor authentication where one factor is provided by a device separate from the computer gaining access. (See Chapter 2, paragraph 13)
- b. **Access Control.** In accordance with DOJ IT Security Standard – Access Control (AC) Control Family, Component IT systems shall:
- (1) Limit IT system access to authorized users, processes acting on behalf of authorized users, or devices (including other IT systems) and to the types of transactions and functions authorized users are permitted to exercise.
 - (2) Restrict remote access to Government or contractor owned systems. Remote access from personally owned and “public computers” is prohibited. (See Chapter 2, paragraph 13)

- (3) Prohibit automatic forwarding of email received in a Component or Department email system to or through a non-Department email system, unless the Authorizing Official grants a waiver.
- c. **Audit and Accountability.** In accordance with DOJ IT Security Standard – Audit and Accountability (AU) Control Family, Component IT systems shall:
- (1) Create, protect and retain IT system audit records to the extent needed to enable security monitoring, analysis, investigation and reporting of unlawful, unauthorized or inappropriate IT system activity.
 - (2) Ensure the actions of individual IT system users can be uniquely traced to those users so they can be held accountable for their actions.
 - (3) Provide direct, real-time or near real-time electronic data feeds of all relevant security monitoring and auditing data (e.g., Firewall event logs, Intrusion Detection or Prevention system alerts and logs, network and desktop antivirus event logs, content scanning and filtering system logs, DHCP, DNS, etc.) to the Department Security Operations Center (SOC) systems unless the Department CIO grants a waiver based upon assessed risk, mitigating controls and operation requirements.
- d. **System and Communications Protection.** In accordance with DOJ IT Security Standard – System and Communications Protection (SC) Control Family:
- (1) All connections to external networks supporting external access and/or remote access to Department or Component IT systems shall be obtained through a Trusted Internet Connection Access Provider (TICAP), unless the Department CIO grants a waiver based upon assessed risk, mitigation controls and operational requirements.
 - (2) The Department shall maintain and publish a list of known malicious resources and sites. Components shall implement blocking of these resources and sites at boundary protection devices. Exceptions to allow access to resources and/or sites on this list must be approved by the Component CIO and reported to the Department’s Security Operations Center.
 - (3) Components shall monitor, control and protect Component communications (e.g., information transmitted or received by Component IT systems) at the external boundaries and key internal boundaries of the IT systems.
 - (4) Component systems shall utilize approved cryptographic mechanisms or protected distribution systems to protect the confidentiality and integrity of information transmitted beyond the secured physical perimeter.
 - (5) Remote access computers shall use an encrypted VPN to connect to Component information systems.

(6) Components shall employ architectural designs, software development techniques and systems engineering principles that promote effective IT security within Component IT systems.

(7) Components shall be prohibited from deploying systems, technologies, or services (e.g., encapsulation, tunneling, encryption) inconsistent with department security enterprise architecture requirements (e.g., Firewalls, Intrusion Detection Systems, Antivirus systems, content scanning and filtering systems), unless the Department CIO grants a waiver based upon assessed risk, mitigating controls, and operational requirements, prior to operational use.

6. National Security Systems and Sensitive Compartmented Information (SCI) IT Systems

Security policy for systems processing collateral (i.e., non-SCI) national security information is established by the Committee on National Security Systems (CNSS). Security policy for systems processing Sensitive Compartmented Information (SCI) is established by Director of National Intelligence (DNI) in Intelligence Community Directive (ICD) 503, Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation. The Department Security Officer (DSO) is responsible for obtaining accreditation of IT systems processing SCI.

Components shall conform to DOJ Security Program Operating Manual (SPOM), ICD 503 and CNSS policies to manage the security of their National Security Systems. Components shall use NIST SP 800-59, "Guideline for Identifying an Information System as a National Security System," to identify National Security Systems.

7. Classified Laptop and Mobile Computing Devices

The Department Security Officer (DSO) and Department Chief Information Officer (CIO) shall approve, in writing, the processing of classified information on laptops and mobile computing devices. Requests for approval shall be submitted through the Chief Information Security Officer who will obtain the approvals. DOJ IT Security Standard – Classified Laptop and Standalone Computers Security Policy outlines the requirements for laptop computers that process or store classified information, including requirements for standalone computers that process or store classified information.

8. Use of DOJ IT Resources Outside US Territory.

The Department Security Officer (DSO) and Department Chief Information Officer (CIO) shall approve, in writing, the transportation or use of DOJ computers outside of US Territory. Components may approve the use of Department telephones, including BlackBerry smartphones and similar devices, outside US Territory. Components shall:

- a. Limit data taken outside US Territory to that which is needed to accomplish the purpose of the travel.
- b. Prevent remote access to DOJ IT systems from outside US Territory, with the exception of systems specifically accredited for such access and email via smartphones or personal digital assistants (PDAs).
- c. Inspect computers, smartphones, PDAs and media that have been transported outside US Territory for compromise prior to any physical connection to a Component or Department system. If the Component can not conduct such an inspection, it shall reimagine the computer or sanitize the media.

9. Facsimile

- a. All classified and sensitive facsimile transmissions shall be preceded by a cover sheet containing the following information:
 - (1) The classification or sensitivity of the information.
 - (2) The name, office and voice/fax telephone numbers for the recipient(s) and sender.
 - (3) A warning banner with instructions to the recipient if the facsimile was received in error.
- b. Classified information shall be encrypted for transmission with National Security Agency (NSA)-approved encryption.

CHAPTER 2. ISSUE-SPECIFIC SECURITY POLICIES

Whereas program policy is intended to address the broad organization wide computer security program, the issue-specific policies in this chapter focus on areas of current relevance and concern to the Department.

10. Sensitive and Personally Identifiable Information (PII)

The term “personally identifiable information” refers to information that can be used to distinguish or trace individuals’ identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, mother’s maiden name, etc. Loss or disclosure of sensitive information not only has a serious negative impact on our law enforcement and other critical functions, but also diminishes the public trust in our operations. There is inherent risk in carrying such data on mobile computers and devices. The purpose of this policy is to compensate for the lack of

physical security controls when information is removed from or accessed from outside the agency location. Components shall:

- a. Reduce the volume of collected and retained PII to the minimum necessary.
- b. Limit access to only those individuals who must have such access.
- c. Categorize sensitive PII and information systems processing such information as moderate or high impact.
- d. Not remove sensitive PII from Component controlled IT systems or facilities unless required (e.g., court filings, debt collection activities).
- e. Log all computer-readable data extracts from databases holding sensitive information and ensure each extract including sensitive data has been erased within 90 days or its use is still required. All DOJ information is considered sensitive information unless designated as non-sensitive by the Component head.
- f. Notify the DOJ Computer Emergency Readiness Team (DOJCERT) of all incidents involving known loss of sensitive data and PII as an Unauthorized Access incident (Category 1) within one hour of discovery. Loss of any data storage devices, such as laptops, flash drives, disks and tapes, should be reported as an Incident under Investigation (Category 6) within the same one hour time frame. DOJCERT will notify the US-CERT and the Department CIO.
- g. Ensure all contracts involving the processing and storage of PII comply with Department policies on remote access and security incident reporting.

11. External Information Systems

External information systems are information systems or components of information systems that are outside of the accreditation boundary established by the Component and for which the Component typically has no direct control over the application of required security controls or the assessment of security control effectiveness. External access includes interconnections between Department IT systems and non-Department IT systems, and between Component IT systems internal to the Department, where there is direct connection of two or more IT systems for the purpose of sharing data and other information resources. External access also includes connections to the Internet.

External access presents both security concerns and resource management issues. The goal of this policy is to ensure Components can effectively, efficiently and safely exchange data with other government and private sector systems, and can utilize resources available on the Internet to accomplish their missions.

Components shall:

- a. Obtain all connections to external networks that support external access and/or remote access through a Trusted Internet Connection Access Provider (TICAP), unless the Department CIO grants a waiver based upon assessed risk, mitigation controls and operational requirements.
- b. Be prohibited from deploying systems, technologies, or services (e.g., encapsulation, tunneling, encryption, etc) inconsistent with department security architecture requirements (e.g., Firewalls, Intrusion Detection or Prevention Systems, Antivirus systems, content scanning and filtering systems, etc.), unless the Department CIO grants a waiver based upon assessed risk, mitigating controls, and operational requirements, prior to operational use.

12. Protection of Mobile Computers/Devices and Removable Media

Information physically transported outside of the Department's secured physical perimeter is more vulnerable to compromise. The intent of this policy is to compensate for the protections no longer offered by the physical security controls when information is removed from the Component location.

Information on mobile computers/devices (e.g., notebook computers, personal digital assistants) and removable media shall be encrypted using FIPS 140-2 validated or NSA approved encryption mechanism, based on the classification of information processed on the device; unless the data is determined to be non-sensitive, in writing, by the Component Head or principal deputy. Mobile computers shall utilize anti-viral software and a host-based firewall mechanism. Components shall ensure all security related updates are installed on mobile computers/devices. Information should be deleted from mobile computers/devices when no longer needed.

13. Remote Access to DOJ Systems

Remote access is any access to a Component's nonpublic information system by a user (or an information system) communicating through an external, non-Department-controlled network (e.g., the Internet) using a Component controlled computer. Remote access presents additional security concerns since the Component has no direct control over the application of required security controls or the assessment of security control effectiveness of the connecting network. The goal of this policy is to ensure Components can safely utilize remote access to better accomplish their missions.

- a. Remote access systems shall be restricted to Government owned or contractor owned systems. Remote access from personally owned or "public computers" is prohibited.
 - (1) Remote computers shall employ anti-viral software, firewalls and encryption of stored data using FIPS 140-2 validated or NSA approved encryption.

- (2) Remote computers shall have all current and applicable Operating System (OS) and application security updates in place.
- (3) Components shall utilize a configuration management system for remote access computers to ensure the remote access computer has the Component approved security software in place, the OS is fully patched, antivirus software is installed and up-to-date and a personal firewall is enabled.
- (4) Remote access computers shall use two-factor authentication where one factor is provided by a device separate from the computer gaining access.
- (5) Remote access computers shall use an encrypted VPN to connect to Department information systems.
- (6) Remote access computers shall not be connected to any other network when connected to a Department IT system.
- (7) Remote access login sessions shall be restricted to a single operating system and a single network interface card when connected to a Department IT system.

14. Contractors

The Components and Department may utilize contractors to develop, operate and/or maintain IT systems on their behalf. Contractors may be granted access to Component and Department IT systems and information in order to perform work specified under the contract. Access may be from Component or Department owned computers or from contractor owned computers. Contractors may process Component and Department information on contractor owned equipment, either within or outside DOJ space. In all these situations, the contractors and their sub-contractors, their personnel and their IT systems and devices shall fall under the provisions of this order, and the contract shall identify IT security requirements.

All connections to external networks supporting access to DOJ hosted resources (e.g., Government owned web sites, applications, email systems) shall be obtained through a Trusted Internet Connection Access Provider (TICAP), unless the Department CIO grants a waiver based upon assessed risk, mitigation controls and operational requirements.

When the contract requires or allows contractor IT systems to be used, whether to access Component or Department IT systems and/or information or to process or store Component or Department information, the contract shall require the contractor IT systems be certified, accredited and operated pursuant to a valid Authority to Operate (ATO). The ATO shall be issued by a Component Authorizing Official based on this policy. If the contractor utilizes its own internal C&A process it must submit the C&A package to the Component Authorizing Official. If the Component Authorizing Official determines the C&A process

meets the Department standards, he or she may issue an ATO based on the package. Contractors using individual devices under the contract shall provide the Contracting Officer's Technical Representative (COTR) an inventory of such devices and shall operate such devices pursuant to this policy, including all incident response requirements. Contractors and contractor systems shall be subject to the same FISMA data calls as other DOJ systems.

Upon termination of contract work, all DOJ information shall be removed from contractor owned IT equipment. Certification of data removal shall be performed by the contract's project manager and a letter confirming certification shall be delivered to the Contracting Officer within 15 days of the termination of the contract.

CHAPTER 3. DETERMINING SECURITY CONTROL REQUIREMENTS

15. Applicability

The standard security control requirements in this Chapter are applicable to all DOJ IT systems. DOJ IT systems that process National Security Information (NSI) must meet any additional requirements specified by the Committee on National Security Systems (CNSS). DOJ IT systems that process Sensitive Compartmented Information (SCI) must meet any additional requirements specified by the Director of National Intelligence (DNI). If there is a conflict in requirements for systems processing NSI or SCI, the CNSS or DNI requirements shall govern. Components shall use NIST SP 800-59, "Guideline for Identifying an Information System as a National Security System," to identify National Security Systems.

16. Categorize information types and information systems

- a. Components shall categorize all Department IT systems as low-impact, moderate-impact, or high-impact, in accordance with Federal Information Processing Standards (FIPS) 199 and 200, or applicable standards for national security systems, as partially implemented in the Department-approved Cyber Security Assessment and Management (CSAM) Toolkit. This process establishes security categories for information types and information systems. The security categories are based on the potential impact on a Component should certain events occur that jeopardize the information and information systems needed by the Component to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions and protect individuals. The impact value for a system shall be the highest value (i.e., high water mark) from those determined for each type of information resident on the system.
- b. The Component's risk assessment (threat and vulnerability information) and mission criticality indicators are given manual consideration regarding any required adjustments in the categorization results. Rationale for deviations from the recommended security categorizations must be documented in the System Security Plan. Designated senior-level

officials within the Component shall review and approve the security categorizations. Documented results of this approval are captured in the System Security Plan.

17. Select, tailor and supplement initial baseline security controls

- a. The Department has developed IT Security Standards based on the security control families outlined in Federal and National standards, supplemented with additional Department standards. The Department's IT Security Standards outline, in specific detail, the requirements for achieving the high-level goals within this Order. The DOJ IT Security Standards represent minimum DOJ IT security control requirements, supplement this Order and are required for use in accordance with the terms and conditions expressed in the Standards. The requirements in the Standards are implemented in CSAM.
- b. Subsequent to the security categorization process, Components shall select an appropriate set of security controls and assurance requirements for their information systems that satisfy the minimum security requirements set forth in these standards and are tailored (enhanced or limited) based on the results of a risk assessment and local conditions, including Component- or system-specific security requirements, specific threat information, cost-benefit analyses, or special circumstances.
- c. The information system authorizing official shall determine if the control set in the information system security plan is appropriate for securing the information system to an acceptable level of operational risk to the Component. Components shall document the authorizing official's approval of the initial set of tailored security controls in the System Security Plan, including the Component's rationales for any refinements or adjustments to the baseline set of controls.

18. Implement security controls

Components shall then implement the security controls in the information system in accordance with the System Security Plan. Authorizing officials are better positioned to make mission risk determinations based on the known vulnerabilities remaining in the information system after the implementation of an agreed-upon set of security controls.

19. Assess and Authorize the implemented controls

Components shall assess the security controls using appropriate methods and procedures (e.g., CSAM) to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting the security requirements for the system. The system authorizing official shall authorize the information system operation based upon a determination of the risk to Departmental operations and assets, individuals, other organizations, and the Nation resulting from the operation of the information system and the decision that this risk is acceptable.

20. Monitor

- a. Components shall monitor the information system on a continuous basis for changes to the information system or its operational environment, the information system security plan boundaries, or other conditions (e.g., threat and risk factors), conducting security impact analyses of the associated changes, updating the information System Security Plan (and other relevant information system documentation as appropriate) and report changes to the security status of the system to appropriate officials on a regular basis.
- b. Significant changes to the system require reaccreditation by the information system's Authorizing Official. Examples of changes to an information system that should be reviewed for possible reaccreditation include:
 - (1) installation of a new or upgraded operating system, middleware component, or application;
 - (2) modifications to system ports, protocols, or services;
 - (3) installation of a new or upgraded hardware platform or firmware component; or
 - (4) modifications to cryptographic modules or services;
 - (5) additional connections to information systems outside the accreditation boundary;
 - (6) functional changes or enhancements to the system that affect its mission criticality, information types, user base, or classification of data supported by the information system.
- c. Changes in laws, directives, policies, or regulations, while not always directly related to the information system, can also potentially affect the security of the system and trigger a reaccreditation action.
- d. Reauthorization should be avoided in situations where the continuous monitoring process provides the necessary and sufficient information to authorizing officials to manage the potential risk arising from the information system changes.

CHAPTER 4. ROLES AND RESPONSIBILITIES

21. Department Chief Information Officer

Per the Clinger Cohen Act of 1996, the Chief Information Officer (CIO), who also serves as Deputy Assistant Attorney General, Information Resources Management (DAAG/IRM), advises and assists the Attorney General, the Deputy Attorney General, the Assistant Attorney General for Administration and other senior staff in order to ensure the Department

plans, acquires, manages and uses Information Technology (IT) in a manner that enhances mission accomplishment; improves work processes and reduces paperwork; provides sufficient protection for the privacy of personal information; promotes citizen-centered electronic government; and is consistent with all applicable Federal laws and directives. The Department CIO, in addition to the responsibilities outlined in Department Order 2880.1B, Information Resources Management Program, shall be responsible for:

- a. Ensuring the Department's IT security program is established and implemented in compliance with Federal laws and regulations.
- b. Issuing IT security policy, standards and guidelines to address IT security planning, management and implementation.
- c. Developing and/or managing enterprise IT control techniques and technologies while considering Department Component infrastructure and resources and developing and/or managing enterprise security management tools.
- d. Reviewing and evaluating the implementation of Department Component program and system security controls in accordance with Department's IT security policy, standards and guidelines.
- e. Developing and maintaining the Department's IT Security Program Management Plan (PMP) in accordance with Federal laws and regulations.
- f. Developing, implementing and managing a Department-wide Plan of Action and Milestone (POAM) process to correct IT security weaknesses.
- g. Requiring Components and program officials to implement Department policy, standards and guidance in the absence of an approved waiver (where applicable), or justification for the use of compensating controls, including a formal assessment and acceptance of risk.
- h. Ensuring senior agency officials provide IT security protections commensurate with the risk and magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of:
 - (1) Information collected or maintained by or on behalf of the Department.
 - (2) IT systems used or operated by an agency, or by a contractor of an agency, or other organization on behalf of an agency.
- i. Enforcing Department IT security policy, including levying sanctions on Components for non-compliance.

- j. Developing and maintaining a central repository of information on new and emerging technologies. Coordinating and approving any evaluations of new and emerging technologies by Components.
- k. Coordinating with the Department Security Officer (DSO) on Sensitive Compartmented Information (SCI) IT systems.
- l. Ensuring all Department personnel with access to Department networks and all individuals at contractor facilities working on Department systems, information, or providing services, receive annual IT security awareness training.
- m. Ensuring IT security management processes are integrated with the Department and/or Component strategic and operational planning processes.
- n. Concurring with or disapproving waiver requests relating to non-United States (U.S.) citizens accessing or assisting in the development, operation, management, or maintenance of Department IT systems.
- o. Approving and monitoring waivers to IT security requirements (other than waivers relating to non-U.S. citizens accessing or assisting the development, operation, management, or maintenance of Department IT systems).
- p. Approving encryption technologies that are not FIPS 140-2 validated in those situations where FIPS-validated products are not available.
- q. Appointing a Chief Information Security Officer (CISO) to carry out the Department-wide IT security program as required by the Federal Information Security Management Act (FISMA).
- r. Establishing an IT Security Governance Committee (ITSGC) to be chaired by the Department CIO and consisting of the Deputy Department CIOs and selected Component CIOs. The ITSGC shall be the focal point for providing strategic direction on Department level initiatives.
- s. Establishing an IT Security Council (ITSC) with supporting project teams composed of lead-Component IT security personnel.
- t. Reporting to the Attorney General and Office of Management and Budget (OMB) on the status of the Department's IT Security Program.

22. Chief Information Security Officer

The Chief Information Security Officer (CISO) chairs the Department's ITSC and serves as the principal security leader for the Department to implement the requirements of FISMA. The CISO also serves as the Department CIO's liaison to Federal agencies for all matters

relating implementation of IT security and the Department's IT Security Program. The Department CISO shall be responsible for:

- a. Developing standards and guidelines for conducting risk assessments to assess risk and determine needs.
- b. Implementing Department-wide policy and procedures for related controls to cost-effectively reduce risks to an acceptable level.
- c. Monitoring, evaluating and periodically testing IT security controls and techniques to ensure they are effectively implemented.
- d. Developing and maintaining a Department-wide IT security program.
- e. Providing leadership for the ITSC to execute Department-wide management and implementation of the Department's IT security program.
- f. Identifying and developing common security controls and managing the implementation and assessment of common security controls.
- g. Ensuring and promoting a comprehensive IT security training program for both privileged and general users.
- h. Assessing waiver requests for Department's IT Security Standards on behalf of the Department Chief Information Officer (CIO).
- i. Preparing the annual and quarterly Federal Information Security Management Act (FISMA) reports for the Department CIO.
- j. Ensuring compliance with monthly reporting on the effectiveness of Component IT security programs, including progress of remedial actions.
- k. Identifying IT security management and reporting tools through the IT Security Council (ITSC) for use throughout the Department.
- l. Assisting senior Department Component IT security officials in their responsibilities through the ITSC.

23. Department Security Officer

The Department Security Officer (DSO) conducts security compliance reviews to assess the overall effectiveness of security program implementation across the Department, including IT security. The DSO ensures all IT security reviews that require system testing are coordinated with the Department CIO and all IT security-related findings are reported to the Department CIO. The DSO shall be responsible for:

- a. Providing advice to the Department CIO on security program areas affecting IT.
- b. Providing advice and recommendations to the Department CIO on waiver requests.
- c. Concurring with or disapproving requests for waivers relating to non-United States (U.S.) citizens accessing or assisting in the development, operation, management, or maintenance of Department IT systems.
- d. Ensuring the development and implementation of Department-wide policy and procedures to govern: TEMPEST; Technical Surveillance Countermeasures (TSCM); Personnel Security; Physical and Environmental Security; Storage and Marking; Media Disposal; Media Reuse; Communications Security (COMSEC) materials; facsimile security; copier security; and those aspects of the DSO's responsibilities for Personnel Security; Document Security; Physical Security; COMSEC; and Emergency Planning described in Department Order 2600.2C.

24. Component Heads or Their Designee(s)

The Component Head or his/her designee(s) shall establish and maintain a Component-wide IT security program to secure the Component's IT systems, networks and data in accordance with Department policy, procedures and guidance. The Component Head or designee(s) work with the Department Chief Information Security Officer (CISO) through the IT Security Governance Committee and IT Security Council to carry out the following responsibilities at the Component level:

- a. Implementing Department policy, standards and guidelines.
- b. Implementing the Department's IT Security Program Management Plan at Component and system level, and reporting results in accordance with Office of the CIO (OCIO) guidelines.
- c. Ensuring the completion of monitoring, testing and evaluation of the effectiveness of IT security policy, procedures, practices and security controls to be performed with a frequency depending on risk, as directed by ITSS.
- d. Ensuring the completion of periodic assessments of risk, including the magnitude of harm that could result from unauthorized access, use, disclosure, disruption, modification, or destruction of information and IT systems that support the operations and assets of the Department.
- e. Developing, implementing, managing and prioritizing corrective plans of actions and milestones to correct known weaknesses in IT security using the department-wide POAM process.

- f. Reporting quarterly in accordance with guidance issued by Justice Management Division (JMD) or the Department CIO, on the status of their IT security programs to the Department CIO and CISO.
- g. Integrating security in the Capital Planning Investment Control (CPIC) process.
- h. Assigning roles and responsibilities within the Component (e.g., Component ITSC member, Component CIO, Authorizing Official, Certification Agent, Information System Owner, Information Owner, User Representative, Information System Security Officer).
- i. Coordinating with the OCIO any evaluations of new technologies that could impact Department or enterprise services.
- j. Participating with other Components and the OCIO in evaluating and selecting IT security tools for use within the Department and obtaining Department CIO approval for non-enterprise IT security solutions.
- k. Establishing procedures to ensure software installed on Component IT systems is in compliance with applicable copyright laws and is incorporated into the IT system's life cycle management process.
- l. Approving, with the concurrence of the Department CIO and Department Security Officer (DSO), waivers relating to non-United States (U.S.) citizens accessing or assisting in the development, operation, management, or maintenance of Department IT systems, and monitoring those waivers.
- m. Ensuring all Component personnel with access to Department networks and all individuals at contractor facilities working on Department systems, information, or providing services, receive annual IT security awareness training.

CHAPTER 5. AGENCY-WIDE PROGRAM IMPLEMENTATION

25. Core Program

- a. The Department shall develop and manage an agency-wide IT Security Program, executed through the Department's IT Security Program Management Plan (PMP), consistent with the laws and regulations affecting IT security. The Department's IT security management approach shall employ a collaborative and coordinated effort to maximize available resources and protect Department IT systems and operations.
- b. The Department Chief Information Officer (CIO) shall establish security governance through the use of appropriate committees to provide a systematic forum to assist in the accomplishment of established Department IT security objectives.

26. IT Security Management Strategy

The IT security management strategy used by the Department shall be based on the risk management concepts found in Office of Management and Budget (OMB) Circular A-130, Appendix III, "Security of Federal Automated Information Systems," the Federal Information Security Management Act (FISMA), and other Federal guidance. The risk management principles in the proceeding sections provide the framework for the Department's IT security management strategy. An important factor in effectively implementing these principles is linking them in a cycle that ensures IT security policy addresses current risks on an ongoing basis.

a. Central Focal Point

The Information Technology Security Staff (ITSS) shall serve as the central focal point for IT security in the Department. The ITSS shall provide Department-wide management and implementation of the Department IT security program. The ITSS and the Components shall provide a collaborative team to manage the accomplishment of priorities for achieving business objectives and complying with FISMA; Homeland Security Presidential Directives; Presidential Decision Directives/ Presidential Directives; Executive Orders; Office of Management and Budget (OMB); National Institute of Standards and Technology (NIST); Committee on National Security Systems (CNSS); Director of National Intelligence (DNI) Directives; and Department IT security requirements.

b. Follow a Department-wide common Security Strategy

The Department shall follow a common Security Strategy that defines the common security goals for all Components. These goals shall outline the Department's security posture both internally and externally while taking into account the respective business needs and missions of each Component. The Department's common Security Strategy will be strengthened by the adoption of a common IT Security Architecture developed to ensure information systems remain secure throughout their entire lifecycle. The security needs and requirements shall be identified early on in the process and be funded appropriately.

c. New and emerging technologies

Information technology is a dynamic field with new and emerging technologies constantly being identified that could assist the Department to better accomplish its constantly evolving mission. The OCIO shall provide a central repository of information on these technologies. Components shall coordinate with this office prior to undertaking any evaluation of new or emerging technologies. This office shall maintain all evaluations and make them available to Components to leverage work already performed and to avoid duplication of effort.

d. Implement Policy and Procedures

- (1) The Department's IT Security policy shall clearly address the Department's IT security needs and serve as the foundation for the Department's IT security program. Policy shall represent the primary mechanism for senior management to communicate its IT security requirements to the Components. Policy shall be adjusted (as required) and shall be related to the risk of the Department or Components not being able to perform their functions.
- (2) The Department's IT Security Standards shall provide detailed procedures for implementing Department policy and shall be practical to implement. The IT Security Standards shall outline specific requirements for accomplishing the Department's security goals. The Department's IT Security Standards are divided into the following three general security control classes: (i) Management; (ii) Operational; and (iii) Technical.

e. Promote Awareness

All users of Department IT systems shall be continually educated on risks and related policy as they are more likely to support and comply with the policy if they understand the purpose behind the policy and their associated responsibilities.

f. Manage Risk and Determine Needs

- (1) Senior management views IT security as an "enabler." Based on a thorough examination of the risks, Department and Component Senior management shall assume risks and take responsibility for the operation of systems based on risks identified in assessments balanced by the impact the IT system has on Department operations. Additionally, the risk management process shall be continually evaluated to ensure it addresses the current threats to Department IT systems.
- (2) The Department's risk management methodology shall present a formal, structured approach for developing risk assessments for IT systems that are part of a major application or general support system. This methodology shall provide a uniform standard for evaluating IT security risks to IT systems operating within the Department. The primary focus of this methodology shall be on the IT system's mission, not IT assets. Since risk management is an essential management function, Department IT system owners and IT security managers shall use this methodology when assessing risks and prioritizing resources for certifying and accrediting Department IT systems.

g. Monitor and Evaluate

The Department's IT security program shall include continually monitoring and assessing IT security policy and IT security controls to ensure they remain appropriate and effective. Monitoring control effectiveness and compliance with policy shall be

incorporated within the cycle of managing the Department's IT security program, and shall be performed through the use of automated software tools when possible.

APPENDIX 1. REFERENCES

The following references are applicable to the Department IT security policy. Unless otherwise stated, all references to publications (e.g., NIST Federal Information Processing Standards, NIST Special Publications) are to the most recent version of the referenced publication.

1. Congressional Mandates

- a. Clinger Cohen Act of 1996, (Pub. L. 104-106, 110 Stat. 186); and (Pub. L. 104-208, 110 Stat. 3009).
- b. Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1030.
- c. Computer Security Act of 1987, 15 U.S.C. § 272, 278h, 278g-3, 278g-4.
- d. Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2511.
- e. E-Government Act of 2002, PL 107-347, 44 U.S.C. Ch 35.
- f. Federal Information Security Management Act of 2002 (FISMA), Pub. L. 107-347, 116 Stat. 2899.
- g. Federal Managers Financial Integrity Act of 1982 (FMFIA), Pub. L. 97-255, 96 Stat. 814.
- h. Freedom of Information Act (FOIA), 5 U.S.C. § 552.
- i. Paperwork Reduction Act of 1995 (PRA), Pub. L. 104-13, 109 Stat. 163; 44 U.S.C. 3501-3520.
- j. Privacy Act of 1974, 5 U.S.C. § 552a.

2. Federal/Departmental Regulations/Guidance

- a. 28 C.F.R. 45.4, Personal Use of Government Property.
- b. 36 C.F.R. 1194, Electronic and Information Technology Accessibility Standards (65 FR 80500).
- c. 41 C.F.R. 101-35, Telecommunications Management Policy.
- d. Committee on National Security Systems Instruction (CNSSI) No. 7000, TEMPEST Countermeasures for Facilities.
- e. CNSS Policy (CNSSP) No. 6, National Policy on Certification and Accreditation of National Security Telecommunications and Information Systems
- f. CNSSI No. 4009 National Information Assurance Glossary.
- g. CNSSI No. 4016, National Information Assurance Training Standard For Risk Analysts
- h. CNSS NSS Instruction 1199, Security Categorization for National Security Systems and Information (ODNI/CIO Draft).
- i. CNSS NSS Instruction 1218 (ODNI/CIO Draft), Guide for Developing Security Plans for National Security Information Systems.
- j. CNSS NSS Instruction 1230 (ODNI/CIO Draft), Risk Management Guide for National Security Information Technology Systems, provides guidance on the assessment and mitigation of risk as part of an overall risk management process.
- k. CNSS NSS Instruction 1237 (Draft), Guide for the Security Certification and Accreditation of National Security Information Systems, provides guidance on the security authorization of NSSs.

- l. CNSS NSS Instruction No. 1253 (ODNI/CIO Draft), Security Control Catalog for National 9 Security Systems.
- m. CNSS NSS Instruction 1253A (Draft), Guide for Assessing the Security Controls in National Security Information Systems, provides guidance for determining the effectiveness of security controls.
- n. CNSS NSS Instruction 1260 (Draft), Security Categorization of National Security Information and Information Systems.
- o. DCID 6/5, Policy for Protection of Certain Non-SCI Sources and Methods Information (SAMI).
- p. DCID 6/9, Manual for Physical Security Standards for Sensitive Compartmented Information Facilities (SCIFs).
- q. Department of Justice (DOJ) Order 2600.2C, Security Programs and Responsibilities.
- r. DOJ Security Program Operating Manual (SPOM).
- s. DOJ Order 2610.2A, Employment Security Regulations. Government Paperwork Elimination Act, 44 USC 3504.
- t. DOJ Order 2880.1B, Information Resources Management.
- u. DOJ Order 2740.1, Use and Monitoring of DOJ Computers and Computer Systems.
- v. Federal Information Processing Standard (FIPS) Publication 140-2, Security Requirements for Cryptographic Modules.
- w. FIPS Publication 199, Standards for Security Categorization of Federal Information Systems.
- x. FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems.
- y. FIPS Publication 201-1, Personal Identity Verification (PIV) of Federal Employees and Contractors.
- z. Federal Continuity Directive 1 (FCD 1), Federal Executive Branch National Continuity Program and Requirements.
- aa. Intelligence Community Directive Number 503, Intelligence Community Information Technology Systems Security, Risk Management, Certification and Accreditation.
- bb. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-12, An Introduction to Computer Security: The NIST Handbook.
- cc. NIST SP 800-14, Generally Accepted Principles and Practices for Security Information Technology Systems.
- dd. NIST SP 800-16, Information Technology Security Training Requirements.
- ee. NIST SP 800-18, Guide for Developing Security Plans for Information Technology Systems
- ff. NIST SP 800-27, Engineering Principles for Information Technology Security.
- gg. NIST SP 800-28, Guidelines on Active Content and Mobile Code.
- hh. NIST SP 800-30, Risk Management Guide for Information Technology Systems.
- ii. NIST SP 800-34, Contingency Planning Guide for Information Technology Systems.
- jj. NIST SP 800-35, Guide to Information Technology Security Services.
- kk. NIST SP 800-36, Guide to Selecting Information Technology Security Products.
- ll. NIST SP 800-37, Guide for the Security Certification and Accreditation for Federal Information Systems.
- mm. NIST SP 800-39, Managing Risk from Information Systems.

- nn. NIST SP 800-40, Creating a Patch and Vulnerability Management Program.
- oo. NIST SP 800-41, Guidelines on Firewalls and Firewall Policy.
- pp. NIST SP 800-44, Guidelines on Securing Public Web Servers.
- qq. NIST SP 800-45, Guidelines on Electronic Mail Security
- rr. NIST SP 800-46, Security for Telecommuting and Broadband Communications.
- ss. NIST SP 800-47, Security Guide for Interconnecting Information Technology Systems.
- tt. NIST SP 800-48, Guide to Securing Legacy IEEE 802.11 Wireless Networks.
- uu. NIST SP 800-50, Building an Information Technology Security Awareness and Training Program.
- vv. NIST SP 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations.
- ww. NIST SP 800-53, Recommended Security Controls for Information Systems.
- xx. NIST SP 800-53A, Guide for Assessing the Security Controls in Federal Information Systems.
- yy. NIST SP 800-54, Border Gateway Protocol Security.
- zz. NIST SP 800-55, Security Metrics Guide for Information Technology Systems.
- aaa. NIST SP 800-59, Guideline for Identifying an Information System as a National Security System.
- bbb. NIST SP 800-60 (Vol. I and II), Guide for Mapping Type of Information and Information Systems to Security Categories.
- ccc. NIST SP 800-61, Computer Security Incident Handling Guide
- ddd. NIST SP 800-63, Electronic Authentication Guideline.
- eee. NIST SP 800-64, Security Considerations in the Information System Development Life Cycle.
- fff. NIST SP 800-68, Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist.
- ggg. NIST SP 800-70, Security Configuration Checklists Program for IT Products – Guidance for Checklists Users and Developers.
- hhh. NIST SP 800-76, Biometric Data Specification for Personal Identity Verification.
- iii. NIST SP 800-77, Guide to IPsec VPNs.
- jjj. NIST SP 800-81, Secure Domain Name System (DNS) Deployment Guide.
- kkk. NIST SP 800-83, Guide to Malware Incident Prevention and Handling.
- lll. NIST SP 800-84, Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities.
- mmm. NIST SP 800-88, Guidelines for Media Sanitization.
- nnn. NIST SP 800-92, Guide to Computer Security Log Management.
- ooo. NIST SP 800-94, Guide to Intrusion Detection and Prevention Systems (IDPS).
- ppp. NIST SP 800-95, Guide to Secure Web Services.
- qqq. NIST SP 800-97, Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i.
- rrr. NIST SP 800-100, Information Security Handbook: A Guide for Managers.
- sss. NIST SP 800-111, Guide to Storage Encryption Technologies for End User Devices.
- ttt. NIST SP 800-113, Guide to SSL VPNs.
- uuu. NIST SP 800-114, User's Guide to Security External Devices for Telework and Remote Access.

- vvv. NIST SP 800-115, Technical Guide to Information Security Testing and Assessment.
- www. NIST SP 800-121, Guide to Bluetooth Security.
- xxx. NIST SP 800-123, Guide to General Server Security.
- yyy. NIST SP 800-124, Guidelines on Cell Phone and PDA Security.
- zzz. National Security Agency (NSA)/ Central Security Service (CSS) Policy 9-12, NSA/CSS Storage Device Declassification.
- aaaa. National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 1000, National Information Assurance C&A Process (NIACAP).
- bbbb. National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11, National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products.
- cccc. National Security Telecommunications and Information Systems Security Advisory Memorandum (NSTISSAM) TEMPEST/2-95, RED/BLACK Installation Guidance.

3. Presidential and Office of Management and Budget Guidance

- a. Executive Order 12958, Classified National Security Information, as amended.
- b. EO 12968, Access to Classified Information.
- c. EO 13231, Critical Infrastructure Protection in the Information Age.
- d. EO 13388, Further Strengthening the Sharing of Terrorism Information to Protect Americans.
- e. General Accounting Office (GAO) Federal Information System Control Audit Manual (FISCAM).
- f. International Standard 15408, Common Criteria for Information Technology Security Evaluation.
- g. Homeland Security Presidential Directive (HSPD) 7, Critical Infrastructure Identification, Prioritization, and Protection,
- h. HSPD-12, Policy for a Common Identification Standard for Federal Employees and Contractors.
- i. Memorandum for The Heads of Executive Departments and Agencies, Designation and Sharing of Controlled Unclassified Information (CUI).
- j. National Security Directive 42, National Policy for the Security of National Security and Telecommunications and Information Systems.
- k. National Security Presidential Directive (NSPD 51) / Homeland Security Presidential Directive (HSPD-20), National Continuity Policy.
- l. Office of Management and Budget (OMB) Circular A-127, Financial Management Systems.
- m. OMB Circular A-130, Management of Federal Information Resources (with Appendices and periodic revisions).
- n. OMB Memorandum 99-18, Privacy Policy on Federal Web Sites.
- o. OMB Memorandum 00-13, Privacy Policies and Data Collection on Federal Web Sites.
- p. OMB Memorandum 01-05, Guidance on Inter-Agency Sharing of Personal Data - Protecting Personal Privacy.
- q. OMB Memorandum 04-04, E-Authentication Guidance for Federal Agencies.
- r. OMB Memorandum 04-26, Personal Use Policies and "File Sharing" Technology.

- s. OMB Memorandum 05-02, Financial Management Systems.
- t. OMB Memorandum 06-15, Safeguarding Personally Identifiable Information.
- u. OMB Memorandum 06-16, Protection of Sensitive Agency Information.
- v. OMB Memorandum 06-19, Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments.
- w. OMB Memorandum 07-11, Implementation of Commonly Accepted Security Configurations for Windows Operating Systems.
- x. OMB Memorandum 07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information.
- y. OMB Memorandum 07-18, Ensuring New Acquisitions Include Common Security Configurations.
- z. OMB Memorandum 07-24, Updated Principles for Risk Analysis.
- aa. OMB Memorandum 08-05, Implementation of Trusted Internet Connections (TIC).
- bb. OMB Memorandum 08-16, Guidance for Trusted Internet Connection Statement of Capability Form (SOC).
- cc. OMB Memorandum 08-22, Guidance on the Federal Desktop Core Configuration (FDCC).
- dd. OMB Memorandum 08-23, Securing the Federal Government's Domain Name System Infrastructure.
- ee. OMB Memorandum 08-27, Guidance for Trusted Internet Connection (TIC) Compliance.
- ff. OMB Memorandum 09-02, Information Technology Management Structure and Governance Framework.

Software License Agreement for the IBIS Family of Products

License fees for the IBIS® family of products and all software provided with the system are included in the initial purchase price, and are included in any maintenance fee afterwards, for hardware forming part of the initial purchase or purchased as options.

The following license agreement applies to the purchase and use of the IBIS family of products, whether the units are part of the initial purchase or were purchased as options.

End-User License Agreement

This End-User License Agreement ("Agreement") is entered into by and between Ultra Electronics Forensic Technology Inc. Inc. ("Ultra Electronics Forensic Technology Inc.") and you (either as an individual or as a single legal entity, hereinafter referred to as "Licensee"), for the use of Ultra Electronics Forensic Technology Inc.'s Integrated Ballistics Identification System (IBIS®) family of products. These products include computer software, the media on which the software is delivered (if any), printed materials, and "online" or electronic documentation ("Software"). By using all or any component of the Software, you and your employer if you are an individual, agree to be bound by the terms and conditions of this Agreement. If you do not agree to these terms and conditions, do not use the Software.

1. GRANT OF LICENSE

Ultra Electronics Forensic Technology Inc. hereby grants you a perpetual, limited, non-exclusive, nontransferable, royalty-free license to use Software and associated media and printed materials, if any, and any online or electronic documentation relating thereto solely for your internal business operations. This license is revocable in the event of breach of any condition contained herein. All other rights are reserved to Ultra Electronics Forensic Technology Inc.

2. RESTRICTIONS

The Software is licensed, not sold. Except as expressly provided herein, Licensee may not resell, sublicense, rent, lease, lend, assign or otherwise transfer the Software to a third party. Licensee shall not:

- a. reverse engineer, decompile, or disassemble the Software;
- b. allow timesharing, service bureau, subscription service, or rental use of any third party software provided with the Software;
- c. navigate the underlying data schema;
- d. access or attempt to access directly any software delivered with the IBIS system other than through the IBIS Software, through prepackaged reports or ad hoc reports that are developed by Ultra Electronics Forensic Technology Inc.

Licensee further agrees:

- a. to prohibit publication of any results of benchmark tests run on third party software provided with the Software;
- b. that it will not require the third party or embedded software manufacturers to perform any obligations or incur any liability not previously agreed to between Ultra Electronics Forensic Technology Inc. and such third party or embedded software manufacturer;
- c. to permit Ultra Electronics Forensic Technology Inc. to audit the Licensee's use of the Software and report such use to third party or embedded software manufacturers if so required by their license agreements;
- d. that a third party or embedded software manufacturer may be designated as a third party beneficiary of this Agreement;
- e. if the Licensee is located in the U.S., this transaction excludes the application of the Uniform Computer Information Transactions Act;
- f. that Ultra Electronics Forensic Technology Inc. and any third party and/or embedded software manufacturers retain all ownership and intellectual property rights to the programs;
- g. that some programs may include source code that a third party embedded software manufacturer may provide as part of its standard shipment of such programs, which source code shall be governed by the terms of this Agreement;
- h. that any data transfer will be done through the IBIS software.

The Licensee shall not knowingly transfer, either directly or indirectly, through donation or otherwise, the equipment and/or Software licensed or delivered under the contract, or any product or part thereof, or service which is a direct product of the equipment or software to any party without the prior written consent of Ultra Electronics Forensic Technology Inc. Such transfer would cause Ultra Electronics Forensic Technology Inc. to be in breach of its licensing agreements with third party software manufacturers.

3. SUPPORT SERVICES

Provided a valid maintenance contract is in force, support services for IBIS® are supplied to Licensee as detailed under such maintenance contract.

4. LIMITED WARRANTY

Ultra Electronics Forensic Technology Inc. warrants that it will make commercially reasonable efforts to solve any problem issues.

5. NO OTHER WARRANTIES

FORENSIC TECHNOLOGY MAKES NO WARRANTY THAT THE SOFTWARE CONTAINS NO DEFECTS OR WILL RUN ERROR FREE. EXCEPT AS MAY BE PROHIBITED BY APPLICABLE LOCAL LAW, FORENSIC TECHNOLOGY DISCLAIMS ALL OTHER WARRANTIES AND CONDITIONS WITH REGARD TO THE SOFTWARE, EITHER EXPRESS OR

IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON INFRINGEMENT, AND THE DELIVERY OR THE FAILURE TO DELIVER SUPPORT SERVICES.

6. LIMITATION OF LIABILITY

EXCEPT AS MAY BE PROHIBITED BY APPLICABLE LOCAL LAW, IN NO EVENT SHALL FORENSIC TECHNOLOGY OR ANY THIRD PARTY SOFTWARE MANUFACTURER BE LIABLE FOR ANY SPECIAL, INCIDENTAL, INDIRECT, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, OR ANY OTHER PECUNIARY LOSS) ARISING OUT OF THE USE OF OR INABILITY TO USE THE SOFTWARE OR THE DELIVERY OR FAILURE TO DELIVER SUPPORT SERVICES, EVEN IF FORENSIC TECHNOLOGY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. TERM AND TERMINATION.

Unless this Agreement is terminated under the next sentence, the term of this Agreement shall be perpetual. Without prejudice to any other rights it may have, Ultra Electronics Forensic Technology Inc. may terminate this Agreement by giving notice to you in writing or by electronic communication if you materially breach the terms and conditions of this Agreement.

8. GENERAL PROVISIONS

- 8.1 **LAW TO GOVERN.** This Agreement shall be governed by the laws of Canada.
- 8.2 **ASSIGNMENT OF RIGHTS.** You may permanently assign and transfer all of your rights under this Agreement, provided: (i) you transfer to the recipient the Software and this Agreement, (ii) you retain no copies of the Software; and (iii) the recipient agrees to be bound by the terms and conditions of this Agreement. In the event of permanent assignment and transfer of your rights to another party, you must inform Ultra Electronics Forensic Technology Inc. in writing of such an event, and provide Ultra Electronics Forensic Technology Inc. with the appropriate information on such party.
- 8.3 **TITLES AND SUBTITLES.** The titles and subtitles used in this Agreement are used for convenience only and do not constitute a part of this Agreement.
- 8.4 **SEVERABILITY.** If any provision of this Agreement is held to be illegal or unenforceable, that provision shall be limited or eliminated to the minimum extent necessary so that this Agreement shall otherwise remain in full force and effect and enforceable.
- 8.5 **NON-WAIVER.** No failure by Ultra Electronics Forensic Technology Inc. to take action on account of any default by you shall constitute a waiver of any such default or of the performance required.

- 8.6 **ENTIRE AGREEMENT.** This Agreement, together with any additional conditions in the contract under which the Products were procured, is the sole agreement between you and Ultra Electronics Forensic Technology Inc. with respect to the subject matter hereof. This Agreement supersedes all prior agreements or discussions between you and Ultra Electronics Forensic Technology Inc. with respect to the Software.
- 8.7 **MODIFICATION.** Except as otherwise expressly provided herein, any provision of this Agreement may be amended and the observance of any provision of this Agreement may be waived (either generally or any particular instance and either retroactively or prospectively) only with the written consent of you and Ultra Electronics Forensic Technology Inc.
- 8.8 **COMMERCIAL SOFTWARE LICENSES.** Licensee recognizes that IBIS® uses certain commercial software packages, some of which have been purchased by and licensed to Ultra Electronics Forensic Technology Inc. By using the IBIS product, Licensee is required to accept the transfer of the license agreements and all related terms and conditions of such software programs.
- 8.9 **US GOVERNMENT RESTRICTED RIGHTS:** this computer software is submitted with restricted rights. It may not be used, reproduced, or disclosed by the Government except as provided in paragraph (b)(1) of FAR clause 52.227-19 Commercial Computer Software License (Dec2007) or as otherwise expressly stated in the contract.

Copyright © 2002-2019 Ultra Electronics Forensic Technology Inc. Inc. All Rights Reserved.



City of High Point

Municipal Office Building
211 S. Hamilton Street
High Point, NC 27260

Master

File Number: 2023-224

File ID: 2023-224

Type: Contract

Status: To Be Introduced

Version: 1

Reference:

In Control: City Council

File Created: 05/08/2023

File Name:

Final Action:

Title: Contract - Long Foundation Drilling Co. - Transmission Pole Foundation
City Council is requested to award a contract to Long Foundation Drilling Company in the amount of \$322,276 to relocate a portion of 100kV transmission poles to accommodate the substation rehabilitation work at Jackson Lake Substation.

Notes:

Sponsors:

Enactment Date:

Attachments: 3. Contract – Long Foundation Drilling Co. –
Transmission Pole Foundation

Enactment Number:

Contact Name:

Hearing Date:

Drafter Name: amy.myers@highpointnc.gov

Effective Date:

Related Files:

History of Legislative File

Ver- sion:	Acting Body:	Date:	Action:	Sent To:	Due Date:	Return Date:	Result:

CITY OF HIGH POINT AGENDA ITEM



Title: 100 KV Transmission Pole Foundation Construction
Bid # 9021-042623

From: Tyler Berrier, PE; Electric Utilities Dir.

Meeting Date: May 15, 2023

Public Hearing: N/A

Advertised By: N/A

Attachments: Attachment A: Bid Tabulation
Attachment B: Recommendation Form

PURPOSE:

The Electric Utilities Department has been tasked with relocating a portion of 100kV transmission poles to accommodate the substation rehabilitation work at Jackson Lake Substation. This bid was for the construction of the pole foundations.

BACKGROUND:

This project is a portion of the rehabilitation work being performed at Jackson Lake Substation.

BUDGET IMPACT:

Funds are included in the Capital Budget to cover this service.

RECOMMENDATION / ACTION REQUESTED:

City Staff has reviewed the bid submittal and evaluated the information provided. Staff is recommending that the bid for the 100 kV Transmission Pole Foundation construction be awarded to Long Foundation Drilling Co. Inc. for \$322,276. Long Foundation Drilling Company was the lowest bidder meeting specifications of the 4 bids received.



Bid Tabulation
City of High Point, North Carolina
Jackson Lake Transmission
Bid 9021-042623 / Wednesday, April 26, 2023 PM

Contractor	MWBE	Addendum	Bid Form	Total Bid
Long Foundation Drilling Co	Yes	Yes	Yes	\$322,276.00
GridTech, LLC	Yes	Yes	Yes	\$365,257.00
Quality Plus Services DBA Graves Construction and Drilling Services	No	Yes	Yes	\$436,270.00
Southeastern Power Corporation	Yes	Yes	Yes	\$543,845.55



Southeastern Consulting Engineers, Inc.

April 28, 2023

Mr. Tyler Berrier, P.E.
Electric Utilities Director
City of High Point
P.O. Box 230
High Point, North Carolina 27261

Ref.: Bid No. 9021-042623
Jackson Lake Transmission Line Foundations

Dear Tyler:

The City received informal proposals at 2:00 p.m. on April 26, 2023, from four contractors for the installation of concrete transmission pole foundations. The bids were reviewed for compliance with the specifications and relevant project experience. A bid tabulation is attached.

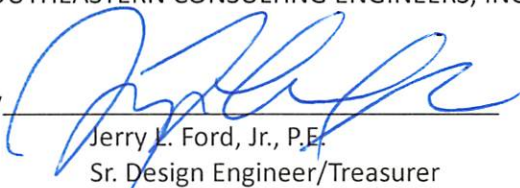
The low bid was submitted by Long Foundation Drilling Company in the amount of \$322,276.00. Long Foundation maintains their corporate headquarters in Hermitage, TN, but also have a local office in Winston Salem, NC. Long Foundation Drilling has been in business since 1985 and has relevant project experience. We believe that Long Foundation Drilling has a thorough understanding of the complexities of the City's project and provided the lowest and most responsive proposal.

We recommend that the City accept Long Foundation Drilling Company's proposal and proceed with executing the contract documents. Please let us know if you have any questions or need any additional information.

Very truly yours,

SOUTHEASTERN CONSULTING ENGINEERS, INC.

By



Jerry L. Ford, Jr., P.E.
Sr. Design Engineer/Treasurer

JLF/lc

Attachment



**FORMAL BID RECOMMENDATION
REQUEST FOR COUNCIL APPROVAL**

DEPARTMENT:

COUNCIL AGENDA DATE:

BID NO.: CONTRACT NO.: DATE OPENED:

DESCRIPTION:

PURPOSE:

COMMENTS:

RECOMMEND AWARD TO: AMOUNT:

JUSTIFICATION:

ACCOUNTING UNIT	ACCOUNT	ACTIVITY	CATEGORY	BUDGETED AMOUNT
TOTAL BUDGETED AMOUNT				

DEPARTMENT HEAD: DATE:

The Purchasing Division concurs with recommendation submitted by the and recommends award to the lowest responsible, responsive bidder in the amount of \$.

PURCHASING MANAGER: DATE:

Approved for Submission to Council
FINANCIAL SERVICES DIRECTOR: DATE:

CITY MANAGER: DATE:



City of High Point

Municipal Office Building
211 S. Hamilton Street
High Point, NC 27260

Master

File Number: 2023-225

File ID: 2023-225

Type: Ordinance

Status: To Be Introduced

Version: 1

Reference:

In Control: City Council

File Created: 05/08/2023

File Name:

Final Action:

Title: Budget Amendment - Agreement - SW Guilford County Fire Hydrant Agreement - High Point Fire Department
City Council is requested to approve an agreement and a budget amendment with Guilford County to fund the installation of eleven (11) Fire Hydrants in Southwest Guilford County.

Notes:

Sponsors:

Enactment Date:

Attachments: 7. Budget Amendment - Agreement – SW Guilford County Fire Hydrant Agreement – High Point Fire Department

Enactment Number:

Contact Name:

Hearing Date:

Drafter Name: amy.myers@highpointnc.gov

Effective Date:

Related Files:

History of Legislative File

Ver- sion:	Acting Body:	Date:	Action:	Sent To:	Due Date:	Return Date:	Result:

CITY OF HIGH POINT

AGENDA ITEM



Title: SW Guilford County Fire Hydrant Agreement

From: Thomas Reid, Fire Chief

Public Hearing: No

Attachments: None

Meeting Date: May 15, 2023

Advertising Date / N/A-

Advertised By:

PURPOSE:

The Fire Department seeks Council approval to enter into an agreement with Guilford County to fund the installation of Fire Hydrants in Southwest Guilford County.

BACKGROUND:

The funds provided through this Agreement will be used to install eleven (11) fire hydrants on to the existing water line that runs from the Randleman Lake to the City of High Point. These hydrant locations were strategically placed in an area of the Pinecroft-Sedgefield Fire District that currently has no pressurized water source. Currently, when there is a fire in this area that needs more water than carried on the fire apparatus, it must be drafted from the nearest pond. The addition of these fire hydrants will drastically improve the water supply operation in the event of a fire in this area.

Of the eleven (11) fire hydrants to be installed, six (6) will be installed on a 30” water main and five (5) will be installed on a 16” water main. In addition to the installation of the hydrants, total project costs include concrete blocking, seeding, traffic control, and hydrant extensions as needed.

BUDGET IMPACT:

The County is providing up to \$200,000 for this project. A budget amendment is attached.

RECOMMENDATION / ACTIONS REQUESTED:

1. High Point Fire Department requests Council’s approval of the attached agreement with Guilford County and that the appropriate City official and/or employee be authorized to execute all necessary documents.
2. High Point Fire Department and Financial Services Department recommends and ask the City Council to approve the attached budget amendment.

Exhibit G: Fire Hydrant Location Map



ID	Address_Lo	Latitude	Longitude
1	Highway 62/Drake Rd	35.921041	-79.85766
2	Highway 62/Tomball Rd	35.91951	-79.865476
3	1072 NC Highway 62 W	35.922301	-79.876871
4	1110 NC Highway 62 W	35.922516	-79.878254
5	1148 NC Highway 62 W	35.925206	-79.885623
6	Highway 62/Groometown Rd. (5766 Groometown Rd)	35.928433	-79.892101

ID	Address_Lo	Latitude	Longitude
7	Hickory Creek Rd/Groometown Rd	35.946895	-79.88803
8	5991 Hickory Creek Rd	35.957544	-79.895427
9	Hickory Creek Rd/Kivett Dr	35.962714	-79.893002
10	Kivett Dr/Chipmunk Dr	35.962259	-79.896413
11	Kivett Dr/Vickrey Chapel Rd	35.962397	-79.89816
0		0	0

OF THE CITY OF HIGH POINT, NORTH CAROLINA
TO APPROPRIATE FUNDS FROM GUILFORD COUNTY
FOR FIRE HYDRANTS IN SOUTHWEST GUILFORD COUNTY

Be it ordained by the City Council of the City of High Point, North Carolina, as follows:

Section 1. The proposed amendment appropriates \$200,000 in funds from Guilford County for the installation of fire hydrants in southwest Guilford County. The locations are in the area of the Pinecroft-Sedgefield Fire District that currently has no pressurized water. The addition of the fire hydrants will improve the water supply operation in the event of a fire in the area.

Section 2. The 2022-2023 Budget Ordinance of the City of High Point should be amended as follows:

(A) That the following Special Revenue Fund revenues be amended as follows:

Guilford County	\$200,000
-----------------	-----------

(B) That the following Special Revenue Fund expenditures be amended as follows:

Fire Hydrant Installation	\$200,000
---------------------------	-----------

Section 3. That all ordinances, or parts of ordinances in conflict with this ordinance are hereby repealed to the extent of such conflict.

Section 4. That this ordinance shall be effective from and after its passage."

Adopted by High Point City Council, this the 15th day of May 2023

Mayor, Jay W. Wagner

ATTEST

Sandra Keeney,
City Clerk

GUILFORD COUNTY CONTRACT NO. [XXXXXX]

American Rescue Plan Act of 2021
Coronavirus State and Local Fiscal Recovery Funds
Agreement
Between
Guilford County, North Carolina
and
City of High Point, North Carolina

Article I. Overview.

Section 1.1. Parties. The parties to this agreement (“Agreement”) are Guilford County, North Carolina, a body politic and political subdivision of the State of North Carolina (“Guilford County”) and City of High Point, North Carolina, a North Carolina municipal corporation (“Awardee”).

Section 1.2. Definitions. The definitions in 2 CFR 200.1 are hereby incorporated into this Agreement.

Section 1.3. Source of Funding. This Agreement is funded by a portion of the \$104,339,752 allocated to Guilford County by the Coronavirus State Local Fiscal Recovery Fund created under section 603 of the American Rescue Plan Act of 2021 (“ARPA/CSLFRF”). More specifically, this project has been identified as Treasury Expenditure Category 6.1 Provision of Government Services.

Section 1.4. Purpose. The purpose of this Agreement is to establish the terms and conditions for an award allocated to the Awardee from Guilford County.

Section 1.5. Term. This Agreement shall govern the performance of the parties for the period June 1, 2023 (the “Effective Date”) through May 31, 2024 (“Expiration Date”), unless earlier terminated by either party in accordance with the terms of this Agreement (“Agreement Term”).

Article II. Scope of Funded Activities.

Section 2.1. Scope of Services. Awardee shall perform all activities described in the scope of activities, attached hereto as Exhibit B (Approved Activities).

Section 2.2. Budget. Awardee shall perform the Approved Activities in accordance with the program budget as approved by Guilford County and attached hereto as Exhibit C (Approved Budget).

Section 2.3. Prior Approval for Changes. Awardee may not transfer allocated funds among cost categories within a budgeted program account without the prior written approval of Guilford County; nor shall Awardee make any changes, directly or indirectly, to program design, Approved Activities, or Approved Budget without the prior written approval of Guilford County.

Article III. Compensation.

Section. 3.1. Payment of Funds. Guilford County agrees to reimburse Awardee for costs actually incurred and paid by Awardee in accordance with the Approved Budget and for the performance of the Approved Activities under this Agreement in an amount not to exceed two hundred thousand dollars (\$200,000.00) (“Total Agreement Funds”). The amount of Total Agreement Funds, however, is subject to adjustment by Guilford County if a change is made in the Approved Activities that affects this Agreement or if this Agreement is terminated prior to the expiration of the Agreement. Program funds shall not be expended prior to the Effective Date or following the earlier of the Expiration Date or the last day of the Agreement Term. Costs incurred shall only be as necessary and allowable to carry out the purposes and activities of the Approved Activities and may not exceed the maximum limits set in the Approved Budget. Expenses charged against the Total Agreement Funds shall be incurred in accordance with this Agreement.

Section. 3.2. Invoices. As full compensation for the Awardee’s delivery of the goods and/or services, and subject to the terms of this Agreement, the County agrees to pay the amounts for the services as set out herein and in Exhibit B, which is attached hereto and incorporated herein by reference. Payment will be made by the County to Awardee within thirty (30) days of receipt of a correct invoice and proper documentation that services have been delivered and provided in accordance with the Agreement. Guilford County may disapprove the requested reimbursement claim. If the reimbursement claim is disapproved, Guilford County shall notify Awardee as to the disapproval. A decision by Guilford County to disapprove a reimbursement claim is final. There is no appeal process for Awardee. If Guilford County approves payment, then Guilford County will disburse the funds without further notice.

Section. 3.3. Guilford County’s Obligations Contingent on Federal Funding and Awardee Compliance. The payment of funds to Awardee under the terms of this Agreement shall be contingent on the receipt and continued availability of such funds by Guilford County from the ARPA/CSLFRF and shall be subject to Awardee’s continued eligibility to receive funds under the applicable provisions of state and federal laws. If the amount of funds that Guilford County receives from the ARPA/CSLFRF is reduced, or the amount of such funds that Guilford County has remaining is insufficient, Guilford County may reduce the amount of funds awarded under this Agreement or terminate this Agreement. Guilford County also may deny payment for Awardee’s expenditures for Approved Activities where invoices or other reports are not submitted by the deadlines specified in this Agreement or for failure of Awardee to comply with the terms and conditions of this Agreement. Guilford County shall have no obligation to pay Awardee any amount in connection with this Agreement except from ARPA/CSLFRF funds.

Article IV. Financial Accountability and Grant Administration.

Section. 4.1. Financial Management. Awardee shall maintain a financial management system and financial records related to all transactions with funds received pursuant to this Agreement. Awardee must administer funds received pursuant to this Agreement in accordance with all applicable federal and state requirements, including those sections of the Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards, 2 CFR Part 200, that apply to ARPA CSLFRF Revenue Replacement Funds. See ARPA/CSLFRF Assistance Listing (21.027); U.S. Department of Treasury CSLFRF Final Rule Frequently Asked Questions 13.15; and Section 5.3 of this agreement. Awardee shall adopt such additional financial management procedures as may from time-to-time be prescribed by Guilford County and/or required by applicable federal or state laws or regulations, or guidelines from U.S. Department of Treasury.

Awardee shall maintain detailed, itemized documentation and other necessary records of all expenses incurred pursuant to this Agreement.

Section. 4.2. Limitations on Expenditures. Guilford County shall only reimburse Awardee for documented expenditures incurred during the Agreement Term that are: (i) reasonable and necessary to carry out the scope of Approved Activities described in Exhibit B; (ii) documented by contracts or other evidence of liability consistent with the established Guilford County and Awardee procedures; and (iii) incurred in accordance with all applicable requirements for the expenditure of funds payable under this Agreement. Guilford County may not reimburse or otherwise compensate Awardee for any expenditures incurred or services provided prior to the Effective Date or following the earlier of the expiration or termination of this Agreement.

Section. 4.3. Indirect Cost Rate. The indirect cost rate, if any, indicated in Exhibit C (Approved Budget) shall apply to this Agreement.

Section. 4.4. Financial and Other Reports. Awardee shall submit to Guilford County such reports and back-up data as may be required by the Federal Government or Guilford County, including such reports which enable Guilford County to submit its own reports to the U.S. Department of Treasury, in accordance with the following schedule, which may be amended from time to time:

<u>REPORT</u>	<u>DEADLINE</u>
Project and Expenditure Reports (Quarterly)	July 31, 2023 October 31, 2023 January 31, 2024 April 30, 2024
Recovery Plan (Annually)	July 31, 2023 July 31, 2024

This provision shall survive the expiration or termination of this Agreement with respect to any reports which the Awardee is required to submit to Guilford County following the expiration or termination of this Agreement.

Section. 4.5. Improper Payments. Any item of expenditure by Awardee under the terms of this Agreement which is found by auditors, investigators, or other authorized representatives of Guilford County, the US Department of Treasury, the NC Department of State Treasurer, or other federal or state instrumentality to be improper, unallowable, in violation of federal or state law, or the terms of this Agreement, or involving any fraudulent, deceptive, or misleading representations or activities of Awardee, shall become Awardee's liability, and shall be paid solely by Awardee, or, if already expended, repaid as directed to Guilford County or the US Department of Treasury, immediately upon notification of such, from funds other than those provided by Guilford County under this Agreement or any other agreements between Guilford County and Awardee. This provision shall survive the expiration or termination of this Agreement.

Section. 4.6. Audits and Access to Records. Awardee certifies compliance with applicable provisions of 2 CFR 200.501-200.521, and continued compliance with these provisions during the term of this section. If Awardee is not required to have a Single Audit as defined by 200.501, US Department of Treasury requirements, or the Single Audit Act, then Awardee shall have a financial

audit performed yearly by an independent Certified Public Accountant. Awardee shall provide notice of the completion of any required audits and will provide access to such audits and other financial information related to the Agreement upon request. Awardee certifies that it will provide Guilford County with notice of any adverse findings which impact this Agreement. This obligation extends for one year beyond the expiration or termination of this Agreement.

Section. 4.7. Closeout. Final payment request(s) under this Agreement must be received by Guilford County no later than thirty (30) days after the earlier of the Expiration Date or the last day of the Agreement Term. Guilford County will not accept a payment request submitted after this date without prior authorization from Guilford County. In consideration of the execution of this Agreement by Guilford County, Awardee agrees that acceptance of final payment from Guilford County will constitute an agreement by Awardee to release and forever discharge Guilford County, its agents, employees, officers, representatives, affiliates, successors and assigns from any and all claims, demands, damages, liabilities, actions, causes of action or suits of any nature whatsoever, which Awardee has at the time of acceptance of final payment or may thereafter have, arising out of, in connection with or in any way relating to any and all injuries and damages of any kind as a result of or in any way relating to this Agreement. The Awardee's obligations to Guilford County under this Agreement shall not terminate until all closeout requirements are completed to the satisfaction of Guilford County. Such requirements shall include submitting final reports to Guilford County and providing any closeout-related information requested by Guilford County by the deadlines specified by Guilford County. This provision shall survive the expiration or termination of this Agreement. By law, Guilford County must expend all ARPA/CSLFRF funds by December 31, 2026. Accordingly, and without extending any earlier deadlines contained in this Section or in this Agreement, Guilford County shall have no obligation to make any payment not made on or before December 31, 2026, and no liability for not making any such payment, regardless of cause.

Article V. Compliance with Grant Agreement and Applicable Laws.

Section. 5.1. General Compliance. Awardee shall perform all Approved Activities funded by this Agreement in accordance with this Agreement, the award agreement between Guilford County and the US Department of Treasury, and all applicable federal, state and local requirements, including all applicable statutes, rules, regulations, executive orders, directives or other requirements. Such requirements may be different from Awardee's current policies and practices. Guilford County may assist Awardee in complying with all applicable requirements. However, Awardee remains responsible for ensuring its compliance with all applicable requirements.

Section. 5.2. Expenditure Authority. This Agreement is subject to the laws, regulations, and guidance documents authorizing and implementing the ARPA/CSLFRF grant, including, but not limited to, the following:

Authorizing Statute. Section 603 of the *Social Security Act* (42 U.S.C. 803), as added by section 9901(a) of the *American Rescue Plan Act of 2021* (Pub. L. No. 117-2); N.C.G.S. §153A-233; §153A-307; and §153A-278.

Implementing Regulations. Subpart A of 31 CFR Part 35 (Coronavirus State and Local Fiscal Recovery Funds), as adopted in the *Coronavirus State and Local Fiscal Recovery Funds* interim final rule (86 FR 26786, applicable May 17, 2021 through March 31, 2022) and final

rule (87 FR 4338, applicable January 27, 2022 through the end of the ARPA/CSLFRF award term), and other subsequent regulations implementing Section 603 of the Social Security Act (42 U.S.C. 803).

Guidance Documents. Applicable guidance documents issued from time-to-time by the US Department of Treasury, including the currently applicable version of the *Compliance and Reporting Guidance: State and Local Fiscal Recovery Funds*.¹

This Agreement is also subject to all applicable laws of the State of North Carolina.

Section. 5.3. Federal Grant Administration Requirements. Without limiting the forgoing, Awardee shall comply with those sections of the *Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards*, 2 CFR Part 200 (UG), as adopted by the Department of Treasury at 2 CFR Part 1000 and as set forth in the Assistance Listing for ARPA/CSLFRF (21.027), that apply to ARPA CSLFRF Revenue Replacement Funds. See US Department of Treasury CSLFRF Final Rule Frequently Asked Questions 13.15. These requirements dictate how Awardee must administer the award and how Guilford County must oversee Awardee.

Applicable UG provisions include:

Subpart A, Acronyms and Definitions

Subpart B, General provisions

Subpart C, Pre-Federal Award Requirements and Contents of Federal Awards (except 2 CFR 200.204, .205, .210, and .213)

Subpart D, Post Federal; Award Requirements (except 2 CFR 200.301, .304-.327, .330-.333, and .339-345)

Subpart E, Cost Principles (except 2 CFR 200.400(d), (f), and (g), .401-.402, .403(b), (e), and (f), .404(a)-(d), and .405-.476)

Subpart F, Audit Requirements

2 CFR Part 25 (Universal Identifier & System for Award Management)

2 CFR Part 170 (Reporting Subaward and Executive Compensation Information)

2 CFR Part 180 (OMB Guidelines to Agencies on Governmentwide Debarment and Suspension (Non-procurement))

2 CFR Part 200, Appendix XII (Recipient Integrity and Performance Matters)

Awardee shall document compliance with UG requirements, including adoption and implementation of all required policies and procedures, within thirty (30) days of the execution of this Agreement and during all subsequent reviews during the term of the Agreement. Guilford County may provide sample policies or other assistance to Awardee in meeting these compliance requirements. Regardless of Guilford County's assistance, it is the Awardee's responsibility to properly comply with all UG requirements as described above. Failure to do so may result in termination of the Agreement by Guilford County.

Section. 5.4. Federal Restrictions on Lobbying. Awardee shall comply with the restrictions on lobbying in 31 CFR Part 21. Pursuant to this regulation, Awardee may not use any federal funds

¹ <https://home.treasury.gov/system/files/136/SLFRF-Compliance-and-Reporting-Guidance.pdf>.

to pay any person to influence or attempt to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with any of the following covered federal actions: the awarding of any federal contract, the making of any federal grant, the making of any federal loan, the entering into of any cooperative agreement, and the extension, continuation, renewal, amendment, or modification of any federal contract, grant, loan, or cooperative agreement. Awardee shall certify in writing that Awardee has not made, and will not make, any payment prohibited by these requirements using the form provided in Exhibit D (Lobbying Certifications).

Section. 5.5. Equal Opportunity & Other Requirements. Awardee shall comply with the requirements in this section.

Civil Rights Laws. Awardee shall comply with Title VI of the Civil Rights Act of 1964 (42 U.S.C. §§ 2000d *et seq.*) and Treasury’s implementing regulations at 31 C.F.R. Part 22, which prohibit discrimination on the basis of race, color, or national origin under programs or activities receiving federal financial assistance.

Fair Housing Laws. Awardee shall comply with the Fair Housing Act, Title VIII of the Civil Rights Act of 1968 (42 U.S.C. §§ 3601 *et seq.*), which prohibits discrimination in housing on the basis of race, color, religion, national origin, sex, familial status, or disability.

Disability Protections. Awardee shall comply with section 504 of the Rehabilitation Act of 1973, as amended (29 U.S.C. 794), which prohibits discrimination on the basis of disability under any program or activity receiving federal financial assistance.

Age Discrimination. Awardee shall comply with the Age Discrimination Act of 1975, as amended (42 U.S.C. §§ 6101 *et seq.*), and Treasury’s implementing regulations at 31 CFR Part 23, which prohibit discrimination on the basis of age in programs or activities receiving federal financial assistance.

Americans with Disabilities Act. Awardee shall comply with Title II of the Americans with Disabilities Act of 1990, as amended (42 U.S.C. §§ 12101 *et seq.*), which prohibits discrimination on the basis of disability under programs, activities, and services provided or made available by state and local governments or instrumentalities or agencies thereto.

Section. 5.6. Federal Funding Accountability and Transparency Act of 2006. Awardee shall provide Guilford County with all information requested by Guilford County to enable Guilford County to comply with the reporting requirements of the *Federal Funding Accountability and Transparency Act of 2006* (31 U.S.C. 6101 note). (See 2 CFR Part 170, Reporting Subaward and Executive Compensation Information.)

Section. 5.7. Licenses, Certifications, Permits, Accreditation. Awardee shall obtain and keep current any license, certification, permit, or accreditation required by federal, state, or local law and shall submit to Guilford County proof of any licensure, certification, permit or accreditation upon request.

Section. 5.8. Publications. Any publications produced with funds from this Agreement shall display the following language: “This project [is being] [was] supported, in whole or in part, by

federal award number SLFRP2097 awarded to Guilford County, North Carolina by the U.S. Department of the Treasury.”

Section 5.9. Program for Enhancement of Contractor Employee Protections. Awardee is hereby notified that they are required to: inform its employees working on any federal award that they are subject to the whistleblower rights and remedies of the program; inform its employees in writing of employee whistleblower protections under 41 U.S.C §4712 in the predominant native language of the workforce; and include such requirements in any agreement made with a subcontractor or subgrantee.

Section 5.10. Prohibition on Certain Telecommunication and Video Surveillance Services or Equipment. Pursuant to 2 CFR 200.216, Awardee shall not obligate or expend funds received under this award to: (1) procure or obtain; (2) extend or renew a contract to procure or obtain; or (3) enter into a contract (or extend or renew a contract) to procure or obtain equipment, services, or systems that uses covered telecommunications equipment or services (as described in Public Law 115-232, section 889) as a substantial or essential component of any system, or as a critical technology as part of any system.

Section 5.11. Use of Name. Neither party to this Agreement shall use the other party’s name, trademarks, or other logos in any publicity, advertising, or news release without the prior written approval of an authorized representative of that party. The parties agree that each party may use factual information regarding the existence and purpose of the relationship that is the subject of this Agreement for legitimate business purposes, to satisfy any reporting and funding obligations, or as required by applicable law or regulation without written permission from the other party. In any such statement, the relationship of the parties shall be accurately and appropriately described.

Section 5.12. Statement of Assurances. Awardee certifies compliance with SF 424B (Statement of Assurances – Non-Construction) and SF424D (Statement of Assurances – Construction).

Section 5.13. Stevens Amendments Requirements. Awardee shall identify that federal assistance funds were used to fund Approved Activities under this Agreement in any publicity and /or signage relating to the funded project or program.

Section. 5.14. Increasing Seat Belt Use. Pursuant to Executive Order 13043, 62 FR 19217 (April 18, 1997), Awardee should encourage its contractors to adopt and enforce on-the-job seat belt policies and programs for their employees when operating company-owned, rented, or personally-owned vehicles.

Section 5.15. Reducing Text Messaging While Driving. Pursuant to Executive Order 13513, 74 FR 51225 (October 6, 2009), Awardee should encourage its employees, Awardees, and contractors to adopt and enforce policies that ban text messaging while driving, and Awardee should establish workplace safety policies to decrease accidents caused by distracted drivers.

Article VI. Cooperation in Monitoring and Evaluation.

Section. 6.1. Guilford County Responsibilities. Guilford County shall monitor, evaluate, and provide guidance and direction to Awardee in the conduct of Approved Activities performed under this Agreement. Guilford County must determine whether Awardee has spent funds in accordance with applicable laws, regulations, including the federal audit requirements and agreements and may monitor the activities of Awardee to ensure that Awardee has met such requirements. Guilford County may require Awardee to take corrective action if deficiencies are found.

Section. 6.2. Awardee Responsibilities.

- (a) **Cooperation with Guilford County Oversight.** Awardee shall permit Guilford County to carry out monitoring and evaluation activities, including any performance measurement system required by applicable law, regulation, funding sources guidelines or by the terms and conditions of the applicable grant award, and Awardee agrees to ensure, to the greatest extent possible, the cooperation of its agents, employees and board members in such monitoring and evaluation efforts. This provision shall survive the expiration or termination of this Agreement.
- (b) **Cooperation with Audits.** Awardee shall cooperate fully with any reviews or audits of the activities under this Agreement by authorized representatives of Guilford County, the North Carolina State Auditor, the US Department of Treasury, and the US Government Accountability Office. Awardee agrees to ensure to the extent possible the cooperation of its agents, employees, and board members in any such reviews and audits. This provision shall survive the expiration or termination of this Agreement.

Section 6.3. Interventions. If Guilford County determines that Awardee is not in compliance with this Agreement, Guilford County may initiate an intervention. The degree of Awardee's performance or compliance deficiency will determine the degree of intervention.

If Guilford County determines that an intervention is warranted, it shall provide written notice to Awardee of the intervention, ordinarily within thirty (30) days of the completion of a report review, desk review, onsite review, audit review, or procedures engagement review or as soon as possible after Guilford County otherwise learns of a compliance or performance deficiency related to the execution of this Agreement. This ordinary time frame shall not limit or prevent Guilford County from acting outside of it. The written notice shall notify Awardee of the following related to the intervention:

- (1) The nature of the additional requirements;
- (2) The reason why the additional requirements are being imposed;
- (3) The nature of the action needed to remove the additional requirement, if applicable;
- (4) The time allowed for completing the actions if applicable; and
- (5) The method for requesting reconsideration of the additional requirements imposed.

Interventions will remain in place until the underlying performance or compliance deficiency is addressed to the sole satisfaction of Guilford County. Guilford County is not limited to the forgoing actions or sequences and may at any time take any lawful actions or remedies.

Section 6.4. Records Retention and Access. Awardee shall maintain all records, books, papers and other documents related to its performance of Approved Activities under this Agreement (including without limitation personnel, property, financial and medical records) through at least December 31, 2031, or such longer period as is necessary for the resolution of any litigation, claim, negotiation, audit or other inquiry involving this Agreement. Awardee shall make all records, books, papers and other documents that relate to this Agreement available at all reasonable times for inspection, review and audit by the authorized representatives of Guilford County, the North Carolina State Auditor, the US Department of Treasury, the US Government Accountability Office, and any other authorized state or federal oversight office.

Section 6.5. Key Personnel. Awardee shall identify all personnel who will be involved in performing Approved Activities and otherwise administering the Agreement, including at least one project manager and one fiscal officer (Key Personnel). Awardee shall notify Guilford County of any changes to these personnel within thirty (30) days of the change. Key personnel names, titles, and contact information are listed in Exhibit F (Key Personnel).

Article VII. Breach and Termination.

Section. 7.1. Termination for Cause. Guilford County may terminate this Agreement for cause after three (3) days written notice. Cause may include misuse of funds, fraud, lack of compliance with applicable rules, laws and regulations, failure to perform on time, or failure to comply with any of the requirements of this Agreement, and shall be determined in Guilford County's sole discretion.

Section. 7.3. Termination by Mutual Agreement. Guilford County and Awardee may agree to terminate this Agreement for their mutual convenience through a written amendment to this Agreement. The amendment will state the effective date of the termination and the procedures for proper closeout of the Agreement.

Section. 7.4. Termination Procedures. If this Agreement is terminated, Awardee may not incur new obligations for the terminated portion of the Agreement after Awardee has received the notification of termination. Awardee must cancel as many outstanding obligations as possible. Costs incurred after receipt of the termination notice will be disallowed. Awardee shall not be relieved of liability to Guilford County because of any breach of Agreement by Awardee. Guilford County may withhold payments to Awardee for the purpose of set-off until the exact amount of damages due Guilford County from Awardee is determined.

Section 7.5. Breach. Without limiting Guilford County's rights to terminate this Agreement, if, through any cause, Awardee shall fail to fulfill its obligations under this Agreement in a timely and/or proper manner ("breach"), either in whole or in part, and such breach has continued for a period of more than thirty (30) days after Guilford County has notified Awardee of such breach, Guilford County shall have all legal, equitable, and administrative rights available under applicable law. Without limiting other remedies, in the event of breach, Guilford County may: Withhold any payment due Awardee for the purpose of setoff until such time as the exact amount of damages due Guilford County from such breach can be reasonably determined (at which time that amount

shall be deducted from any payment(s) otherwise due to Awardee) and/or procure the contracted for services or goods from other sources and hold Awardee responsible for any excess cost occasioned thereby. The filing of a petition for bankruptcy by Awardee shall constitute an act of breach under this Agreement. This section shall not limit any other rights or remedies provided to Guilford County under this Agreement or available to Guilford County under applicable law.

Article VIII. General Conditions.

Section. 8.1. Indemnification. To the extent permitted by law, Awardee agrees to indemnify and hold harmless Guilford County, and any of its officers, agents and employees, and the Federal Government from any claims of third parties arising out of any act or omission of Awardee in connection with the performance of this Agreement (including, without limitation, attorney’s fees and other costs of defense with respect to such claims).

Section. 8.2. Insurance. Awardee must maintain insurance policies with at least the following limits:

<u>Coverage</u>	<u>Minimum Limits</u>
a) Workers’ Compensation	\$500,000 bodily injury per each accident, \$500,000 bodily injury per disease per employee, \$500,000 bodily injury per disease policy limit
b) General Liability	\$1,000,000 per occurrence/\$3,000,000 aggregate
c) Automobile Liability	\$2,000,000 per occurrence

Guilford County may require higher limits if warranted by the nature of this Agreement and the type of activities to be provided. The insurer must provide Guilford County with a Certificate of Insurance reflecting the coverages required in this Section. All Certificates of Insurance shall reflect thirty (30) days written notice by the insurer in the event of cancellation, reduction, or other modification of coverage. In addition to this notice requirement, Awardee must provide Guilford County prompt written notice of cancellation, reduction, or material modification of coverage of insurance. Without limiting any liability it may otherwise have, if Awardee fails to provide such notice, the Awardee assumes sole responsibility for all losses incurred by Guilford County for which insurance would have provided coverage. The insurance policies must remain in effect during the term of this Agreement.

Awardee shall name Guilford County as an additional insured except as to workers compensation insurance and it is required that coverage be placed with an “A” rated insurance company acceptable to Guilford County. If Awardee fails at any time to maintain and keep in force the required insurance, Guilford County may cancel and terminate the Agreement without notice.

Subject to Guilford County’s approval (which shall not be unreasonably withheld), as an alternative to the insurance requirements of this section, Awardee may maintain a program of self-insurance that meets or exceeds these requirements. If this alternative is used, Awardee will provide satisfactory documentation of its self-insurance program to Guilford County upon request.

Section. 8.3. Venue and Jurisdiction. Guilford County and Awardee agree that they executed and performed this Agreement in Guilford County, North Carolina. This Agreement will be governed by and construed in accordance with the laws of North Carolina. The exclusive forum and venue for all actions arising out of this Agreement is the appropriate division of the North Carolina General Court of Justice in Guilford County. Such actions may not be commenced in, nor removed to, federal court unless required by law.

Section. 8.4. Nonwaiver. No action or failure to act by Guilford County constitutes a waiver of any of its rights or remedies that arise out of this Agreement, nor shall such action or failure to act constitute approval of or acquiescence in a breach of this Agreement, except as specifically agreed in writing.

Section. 8.5. Limitation of Guilford County Authority. Nothing contained in this Agreement may be deemed or construed to in any way stop, limit, or impair Guilford County from exercising or performing any regulatory, policing, legislative, governmental, or other powers or functions.

Section. 8.6. Severability. If any provision of this Agreement is determined to be unenforceable in a judicial proceeding, the remainder of this Agreement will remain in full force and effect to the extent permitted by law.

Section. 8.7. Assignment. Awardee may not assign or delegate any of its rights or duties that arise out of this Agreement without Guilford County's prior written consent. Unless Guilford County otherwise agrees in writing, Awardee and all assigns are subject to all Guilford County's defenses and are liable for all Awardee's duties that arise from this Agreement and all Guilford County's claims that arise from this Agreement.

Section. 8.8. Integration. This Agreement contains the entire agreement between the parties pertaining to the subject matter of this Agreement. With respect to that subject matter, there are no promises, agreements, conditions, inducements, warranties, or understandings, written or oral, expressed, or implied, between the parties, other than as set forth or referenced in this Agreement.

Section. 8.9. Notices. All notices and other communications required or permitted by this Agreement must be in writing and must be given either by personal delivery, approved carrier, email, or mail, addressed as follows:

(a) If to Guilford County:
Guilford County Government
Michael Halford
ATTN: Pandemic Recovery Office
301 W. Market St.
Greensboro, NC 27401

(b) If to the Awardee:
City of High Point
ATTN: City Manager's Office
211 S. Hamilton St.
High Point, NC 27261

Section 8.10. No Third-Party Beneficiaries/No Waiver of Immunity.

Awardee and Guilford County acknowledge and agree that there are no intended beneficiaries of this Agreement other than Awardee and Guilford County and that this Agreement does not, and shall not be interpreted to, create rights in any other parties (other than the rights on the part of other governmental units, such as the US Department of Treasury, that are explicitly set forth herein or required by law). Awardee and Guilford County further acknowledge and agree that they reserve all rights, defenses, and immunities that they may have with respect to claims by third-parties that relate in any way to this Agreement or to any act or omission with respect to goods or services related in any way to this Agreement.

Section 8.11. Independent Contractor.

Awardee shall act as an independent contractor for all purposes. Nothing in this Agreement shall be interpreted or construed as creating or establishing the relationship of employer and employee between Guilford County and either Awardee or any agent of Awardee. Awardee is an independent contractor and not an employee, agent, joint venturer, or partner of Guilford County.

Section 8.12 Interlocal Agreement.

In addition to all other applicable laws, regulations, and guidance, this Agreement shall be governed by N.C.G.S. Chapter 160A, Art. 20, Part 1, which authorizes interlocal cooperation and provides that units of local government may enter into interlocal agreements. The purpose of this Agreement is for the Approved Activities, which are determined to be in the best interest of the public safety and welfare of each unit of government’s citizens. In addition to its execution, this Agreement’s effectiveness requires approval by Awardee’s and Guilford County’s governing boards, recorded and spread upon each board’s minutes. Awardee shall employ or contract for the services of all personnel needed to carry out the Approved Activities. Unless provided to the contrary by more specific provision elsewhere in this Agreement, Guilford County’s reimbursements to Awardee under this Agreement shall not cause Guilford County to acquire ownership in any property acquired by Awardee with the reimbursed funds and ownership of such property shall remain with Awardee.

GUILFORD COUNTY

_____ Date
Michael Halford
Guilford County Manager

_____ Date
Robin B. Keller
Guilford County Clerk to Board

[Awardee and successor]

ATTEST:

_____ Date
Greg Ferguson
Deputy City Manager

_____ Date
Sandra Keeney
City Clerk

This instrument has been preaudited in the manner required by the Local Government Budget and Fiscal Control Act.

_____ Date
John Barfield

DRAFT

Exhibit A: Intentionally Omitted

DRAFT

Exhibit B: Approved Activities

Funding Purpose

The funds provided through this Agreement will be used to install eleven (11) fire hydrants on to the existing water line that runs from the Randleman Lake to the City of High Point. These hydrant locations were strategically placed in an area of the Pineroft Sedgefield Fire District that currently has no pressurized water source, please see the map attached hereto as Exhibit G and incorporated by reference. Currently, when there is a fire in this area that needs more water than carried on the fire apparatus, it must be drafted from the nearest pond. The addition of these fire hydrants will drastically improve the water supply operation in the event of a fire in this area.

Of the eleven (11) fire hydrants to be installed, six (6) will be installed on a 30" water main and five (5) will be installed on a 16" water main. In addition to the installation of the hydrants, total project costs include concrete blocking, seeding, traffic control, and hydrant extensions as needed.

Billing Process

This is a cost-reimbursable agreement. Invoices will be submitted to the County by the City of High Point. Subject to and without limiting the other terms of this Agreement, including Article III. Compensation, payment from the County to the City of High Point will be made within thirty (30) days of receipt of accurate and complete invoices including the following:

- Time period the invoice covers
- Service/activity supported by funding
- Brief description of the project progress during the specified time period
- Proper documentation that goods and/or services have been delivered and provided in accordance with this Agreement

Exhibit C: Approved Budget

Consult Guilford County’s Allowable Costs and Cost Principles Policy and the ARPA/CSLFRF Final Rule for specific directives and limitations on cost items.

REVENUES		Total Revenue
Guilford County Coronavirus State and Local Fiscal Recovery Funds Awarded	\$	200,000
Budget Cost Categories		Total Expenditures
1. Personnel (Salary and Wages)	\$	
2. Fringe Benefits	\$	
3. Travel	\$	
4. Equipment	\$	
5. Supplies	\$	
6. Contractual Services and Subawards	\$	
7. Consultant (Professional Service)	\$	
8. Construction	\$	200,000
9. Occupancy (Rent and Utilities)	\$	
10. Research and Development (R&D)	\$	
11. Telecommunications	\$	
12. Training and Education	\$	
13. Direct Administrative Costs	\$	
14. Miscellaneous Costs	\$	
15. Total Costs Federal Grant Funds	\$	200,000
<u>MUST EQUAL REVENUE TOTALS ABOVE</u>		

Exhibit D: Lobbying Certification

The undersigned certifies, to the best of his or her knowledge and belief, that:

1. No Federal appropriated funds have been paid or will be paid, by or on behalf of the undersigned, to any person for influencing or attempting to influence an officer or employee of an agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with the awarding of any Federal contract, the making of any Federal grant, the making of any Federal loan, the entering into of any cooperative agreement, and the extension, continuation, renewal, amendment, or modification of any Federal contract, grant, loan, or cooperative agreement.
2. If any funds other than Federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with this Federal contract, grant, loan, or cooperative agreement, the undersigned shall complete and submit Standard Form-LLL, "Disclosure Form to Report Lobbying," in accordance with its instructions.
3. The undersigned shall require that the language of this certification be included in the award documents for all subawards at all tiers (including subcontracts, subgrants, and contracts under grants, loans, and cooperative agreements) and that all subrecipients shall certify and disclose accordingly.

This certification is a material representation of fact upon which reliance was placed when this transaction was made or entered into. Submission of this certification is a prerequisite for making or entering this transaction imposed by section 1352, title 31, U.S. Code. Any person who fails to file the required certification shall be subject to a civil penalty of not less than \$10,000 and not more than \$100,000 for each such failure.

Signature of Awardee's Authorized Official

Name and Title of Awardee's Authorized Official

Date

Exhibit E: Intentionally Omitted

Exhibit F: Key Personnel

Guilford County INFORMATION	
Administrative Address:	301 W. Market Street Greensboro, NC 27401
Invoice Address:	301 W. Market Street Greensboro, NC 27401
Project Manager Name:	Abby Gostling
Project Manager Title:	Program and Fiscal Recovery Manager
Project Manager Email:	Agostling@guilfordcountync.gov
Project Manager Phone:	336-641-6987
Fiscal Officer Name:	John Barfield
Fiscal Officer Title:	Finance Director
Fiscal Officer Email:	Jbarfield@guilfordcountync.gov
Fiscal Officer Telephone:	336-641-4574
AWARDEE INFORMATION	
Administrative Address:	
Invoice Address:	
Project Manager Name:	
Project Manager Title:	
Project Manager Email:	
Project Manager Telephone:	
Fiscal Officer Name:	
Fiscal Officer Title:	
Fiscal Officer Email:	
Fiscal Officer Telephone:	

Exhibit G: Fire Hydrant Location Map



ID	Address_Lo	Latitude	Longitude
1	Highway 62/Drake Rd	35.921041	-79.85766
2	Highway 62/Tomball Rd	35.91951	-79.865476
3	1072 NC Highway 62 W	35.922301	-79.876871
4	1110 NC Highway 62 W	35.922516	-79.878254
5	1148 NC Highway 62 W	35.925206	-79.885623
6	Highway 62/Groometown Rd. (5766 Groometown Rd)	35.928433	-79.892101

ID	Address_Lo	Latitude	Longitude
7	Hickory Creek Rd/Groometown Rd	35.946895	-79.88803
8	5991 Hickory Creek Rd	35.957544	-79.895427
9	Hickory Creek Rd/Kivett Dr	35.962714	-79.893002
10	Kivett Dr/Chipmunk Dr	35.962259	-79.896413
11	Kivett Dr/Vickrey Chapel Rd	35.962397	-79.89816
0		0	0



City of High Point

Municipal Office Building
211 S. Hamilton Street
High Point, NC 27260

Master

File Number: 2023-226

File ID: 2023-226

Type: Miscellaneous Item

Status: To Be Introduced

Version: 1

Reference:

In Control: City Council

File Created: 05/08/2023

File Name:

Final Action:

Title: Consideration of Funding - Outside Non-Profit Organizations
City Council is requested to finalize recommendation for funding the outside organization requests.

Notes:

Sponsors:

Enactment Date:

Attachments: 8. Consideration of Funding – Outside Non-Profit Organizations

Enactment Number:

Contact Name:

Hearing Date:

Drafter Name: amy.myers@highpointnc.gov

Effective Date:

Related Files:

History of Legislative File

Ver- sion:	Acting Body:	Date:	Action:	Sent To:	Due Date:	Return Date:	Result:

CITY OF HIGH POINT AGENDA ITEM



Title: Consideration of Funding for Outside Non-Profit Organizations

From: Stephen M. Hawryluk
Budget & Performance Manager

Meeting Date: May 15, 2023

Public Hearing: No

**Advertising Date /
Advertised By:** N/A

Attachments: Summary of Requests

PURPOSE:

The Finance Committee is responsible for reviewing outside non-profit organization funding requests to make recommendations to the Council regarding annual funding levels.

BACKGROUND:

Outside non-profit agencies submitted requests in the amount of \$1,991,009 for FY 2023-24. The historic policy has been to allocate 1/3 of one penny of the tax rate to be distributed to the agencies, which is equal to \$446,401 for the upcoming fiscal year.

BUDGET IMPACT:

\$446,401 is budgeted in the proposed FY 2023-24 budget, pending final funding decisions.

RECOMMENDATION / ACTIONS REQUESTED:

City Council is requested to finalize recommendation for funding the outside organization requests.

City of High Point
Outside Non-Profit Organizations
Requests FY 2023-2024

	Agency Name	FY2023 Approved Budget	FY2024 Requested Budget	FY2024 Committee Recommend	FY2024 Approved Budget
1	D-Up Basketball Fundamentals	\$ 15,000	\$ 40,640		
2	Greater High Point Food Alliance	12,000	15,000		
3	Helping Hands High Point Inc	15,000	15,000		
4	High Point Arts Council	80,000	125,000		
5	High Point Discovered	15,000	43,445		
6	High Point Leap	15,000	20,000		
7	High Point Rowing	10,000	-		
8	Macedonia Family Resource Center	22,000	25,000		
9	Open Door Ministries	25,000	50,000		
10	Salvation Army/Boys & Girl Club of HP	15,000	25,000		
11	Theatre Art Galleries	40,000	75,000		
12	Triad Food Pantry	20,000	20,000		
13	West End Ministries	30,000	30,000		
14	YWCA of High Point	30,000	75,000		
15	High Point School Partnership	7,500	18,850		
16	Friends of John Coltrane	10,000	25,000		
17	Piedmont Triad Film Commission	7,000	10,000		
18	Carl Chavis YMCA	45,000	50,000		
19	Operation Xcel	-	36,000		
20	C3 - Community Collaboration for Children, Inc	-	15,000		
21	A Simple Gesture	-	10,000		
22	Hayden-Harman Foundation	-	10,800		
23	The Mind Group	-	100,000		
24	Homegrown Heroes, Inc	-	48,000		
25	Borthers Organized to Serve Others (BOTS0)	-	20,000		
26	Commander Peace Academy, Inc	-	20,000		
27	The Sister Circle International	-	50,000		
28	Lydia House	-	18,274		
29	Puzzle Play	-	1,000,000		
	Subtotal:	\$ 413,500	\$ 1,991,009	\$ -	\$ -



City of High Point

Municipal Office Building
211 S. Hamilton Street
High Point, NC 27260

Master

File Number: 2023-227

File ID: 2023-227

Type: Resolution

Status: Public Hearing

Version: 1

Reference:

In Control: City Council

File Created: 05/08/2023

File Name:

Final Action:

Title: Information Regarding Resolution - SELS USA LLC Project - NC Building Reuse Grant
City Council is requested to consider a request to approve a local match for a State of North Carolina Building Reuse Grant for SELS USA LLC not to exceed \$5,000. A public hearing will be conducted at the May 15, 2023 City Council meeting.

Notes:

Sponsors:

Enactment Date:

Attachments: 9. Resolution - SELS USA LLC Project – NC Building Reuse Grant

Enactment Number:

Contact Name:

Hearing Date:

Drafter Name: amy.myers@highpointnc.gov

Effective Date:

Related Files:

History of Legislative File

Ver- sion:	Acting Body:	Date:	Action:	Sent To:	Due Date:	Return Date:	Result:

CITY OF HIGH POINT AGENDA ITEM



**Title: SELS USA LLC Project – Local Match/State Grant
& Resolution of Support**

From: Sandy Dunbeck, Director
High Point Economic Development

Meeting Date: May 15, 2023

Public hearing: Yes

Advertising Date: May, 4, 2023

Attachments: Legal Notice

Advertised by: HPE

PURPOSE:

The High Point City Council is asked to consider a request to approve a local match and resolution of support for a State of North Carolina Building Reuse Grant for SELS USA LLC. The local match would not exceed \$5,000.

PROJECT & BACKGROUND:

SELS (Smart Era Lighting System) Solar specializes in innovative, efficient, off-grid energy solutions. Their solar-powered products include streetlights, bench charging stations, transit lighting, mobile power units, signs/billboards, garden lights, and more. The SELS building reuse project would allow for in-house assembly of several of their products.

The company has purchased buildings at 1710 and 1720 King St. in High Point, totaling 21,400 square feet, and plans to invest a total of \$921,241 to purchase, renovate, and equip the facilities.

The company will relocate 5 jobs and create 13 new jobs paying above the county average wage over a 3-year period.

BUDGET IMPACT:

Upon the company being awarded the grant, the City would provide an amount not to exceed \$5,000 to the State as the local match. The source of those monies would be the City's Economic Development Incentive Fund, which is funded by general and electric revenues.

RECOMMENDATION / ACTION REQUESTED:

The High Point Economic Development staff recommends that City Council authorize an amount not to exceed \$5,000 as the City's local match for the grant and approve a resolution of Support for the State of NC Building Reuse Grant.

Thursday, May 4, 2023

Pursuant to N.C. General Statute 158-7.1, notice is hereby given that a public hearing will be held on Monday, May 15, 2023, at 5:30 p.m. in the Council Chambers, High Point Municipal Building, 211 S. Hamilton St., High Point, NC. The purpose of the hearing is to receive public input on a respective funding request for a local match for a State of NC Building Reuse Grant for SELS USA LLC. The company expects to expand at 1710 and 1720 King St., High Point, NC, and proposes to relocate 5 full-time jobs and create 13 full-time jobs. The High Point City Council will consider authorizing an amount not to exceed \$5,000 – with the source of funding being the Economic Development Incentive Fund, which is funded by general and electric revenues. The City would be authorized to provide this local match to the company upon the company being awarded the State grant.

**RESOLUTION IN SUPPORT OF THE STATE OF NORTH CAROLINA BUILDING REUSE
GRANT FOR SELS USA LLC OF HIGH POINT EXPANSION IN HIGH POINT, NC**

WHEREAS, the State of North Carolina (“State”) is considering approval of a Building Reuse Grant (“Grant”) in the amount of \$100,000 for SELS USA LLC. (“Company”), which will be received by the City and passed on to the Company along with a City of High Point 5% match, upon performance; and

WHEREAS, the High Point City Council supports the State of North Carolina funding a Building Reuse Grant for the Company which is an assembler and installer of innovative, efficient, off-grid energy solutions.; and

WHEREAS, the funding will allow the company to reactivate vacant buildings located at 1710 and 1720 King St, High Point and create 13 jobs paying above the Guilford County average wages; and

WHEREAS, the State requires that a resolution of support be adopted by the High Point City Council proclaiming its support for the Company and the funding; and

WHEREAS, the City believes that it is in the best interests of the citizens of High Point to encourage and support economic development within the City through the recruitment of new industries to the City and the expansion of existing industries in the City.

NOW, THEREFORE, BE IT AND IT IS HEREBY RESOLVED AS FOLLOWS:

1. The High Point City Council hereby adopts this Resolution of Support for the State of North Carolina to provide a Building Reuse grant to SELS USA LLC for its expansion project in High Point, NC.
2. The Mayor and the City Clerk are hereby authorized to sign all necessary documents on behalf of the City.
3. This resolution shall become effective upon adoption.

This 15th day of May 2023.

ATTEST

Sandra Keeney,
City Clerk

Jay W. Wagner,
City of High Point Mayor



City of High Point

Municipal Office Building
211 S. Hamilton Street
High Point, NC 27260

Master

File Number: 2023-228

File ID: 2023-228

Type: Miscellaneous Item

Status: Public Hearing

Version: 1

Reference:

In Control: City Council

File Created: 05/08/2023

File Name:

Final Action:

Title: Information Regarding Dive Bar - Performance Based Incentives
City Council is asked to consider a request from Dive Bar, to authorize performance-based incentives for a retail project at 312 N. Elm St. in the amount of \$124,798 and authorize the City Manager to execute a performance agreement with the company containing benchmarks for the company to achieve and a schedule for the payment of such financial incentives. A public hearing will be conducted at the May 15, 2023 City Council Meeting.

Notes:

Sponsors:

Enactment Date:

Attachments: 10. Dive Bar – Performance Based Incentives

Enactment Number:

Contact Name:

Hearing Date:

Drafter Name: amy.myers@highpointnc.gov

Effective Date:

Related Files:

History of Legislative File

Ver- sion:	Acting Body:	Date:	Action:	Sent To:	Due Date:	Return Date:	Result:

CITY OF HIGH POINT AGENDA ITEM



Title: Public Hearing for Dive Bar
From: Sandy Dunbeck, Director
High Point Economic Development
Public hearing: Yes
Attachments: Legal Notice

Meeting Date: May 15, 2023

Advertising Date: May 4, 2023

Advertised by: HPE

PURPOSE:

The High Point City Council is asked to consider a request from Dive Bar, to authorize performance-based incentives for a retail project at 312 N. Elm St. in the amount of \$124,798 over a four-year period.

PROJECT & BACKGROUND:

The Dive Bar is a barcade concept that will include pool tables, arcade games, pinball, darts, skeeball, basketball, and more. They exist to bring North Carolina back to the days of simple fun and affordability. Their model is built to serve everyone, as they pride themselves on being family friendly before 8PM and welcome to all. They currently operate locations in Hickory and Mooresville, NC.

The company would create 19 new positions

The company anticipates new real and personal property investment of \$650,000.

The company would lease 4,794 square feet of retail space for seven years with two options to renew for 5 and then 3 years at 312 N. Elm St. across from Truist Point.

BUDGET IMPACT:

The source of those monies would be the City's Economic Development Incentive Fund, which is funded by general and electric revenues.

RECOMMENDATION / ACTION REQUESTED:

The High Point Economic Development staff recommends that City Council authorize performance-based incentives for the project in the amount of \$124,798 and authorize the City Manager to execute a performance agreement with the company containing benchmarks for the company to achieve and a schedule for the payment of such financial incentives.

Pursuant to N.C. General Statute 158-7.1, notice is hereby given that a public hearing will be held by the High Point City Council on Monday, May 15, 2023, at 5:30 p.m. in the Council Chambers, High Point Municipal Building, 211 S. Hamilton Street, High Point, NC, for the purpose of receiving public input on a funding request from a company considering locating at 312 N. Elm St. in High Point, NC. The company proposes leasing 4,794 square feet of space. High Point City Council will consider rental assistance incentives of up to \$124,798 over a four-year period for the project. The source of local funding would be the High Point Economic Development Incentive Fund, which is funded by general and electric revenues. The City would be authorized to provide this financial assistance pursuant to an incentive performance agreement containing benchmarks and a schedule for the payment of such financial assistance. For further information, **103** call 336-883-3116.

May 4, 2023