CITY OF HOLLY HILL, FLORIDA

CITY COMMISSION

AGENDA ● OCTOBER 22, 2024

City Commission Chamber	Regular City Commission Meeting	6:00 PM

CITY HALL
1065 RIDGEWOOD AVENUE
HOLLY HILL, FL 32117

City Clerk's office: (386) 248-9441 - Fax: (386) 248-9448

HOLLY HILL
FLORIDA

City Commission Chamber
City Hall
1065 Ridgewood Avenue
Holly Hill, FL 32117

CITY COMMISSION MEMBERS

Mayor
Chris Via

District 1 - Commissioner
John Penny

District 2 - Commissioner
Penny Currie

District 3 - Commissioner
John C. Danio

District 4 - Commissioner
Roy Johnson

CITY MANAGER
Joseph Forte

CITY CLERK
Valerie Manning

1. CALL TO ORDER

a. Roll Call
b. Invocation by Mayor Chris Via
c. Pledge of Allegiance

2. PRESENTATIONS

A. American Legion Post 120 - Presentation to Mayor Chris Via
B. Government Finance Officers Association - Award of Excellence

1. Government Finance Officers Association - Award of Excellence

   (Requested by Valerie Manning, City Clerk)

3. PUBLIC COMMENTS

4. APPROVAL OF MINUTES

1. Minutes - October 8, 2024 Regular City Commission Meeting

   (Requested by Valerie Manning, City Clerk)

5. CONSENT AGENDA - ITEMS (1 - 8)

The action proposed is stated for each item on the Consent Agenda. Unless a City Commissioner removes an item from the Consent Agenda, no discussion on individual items will occur and a single motion will approve all items. Is there anyone in the audience who wishes to speak on any item on the Consent Agenda?

1. Resolution –2024-R-80 A Resolution of the City Commission of the City of Holly Hill, Florida, Adopting the National Institute of Standards and Technology Cybersecurity Framework and Authorize the Chief Technology Officer to Complete the Local Governance Cybersecurity Standards Attestation Form Via the Florida Digital Service Online Portal Before January 1, 2025 Deadline; Providing for Severability; and Providing for an Effective Date.

   (Requested by Valerie Manning, City Clerk)

2. Resolution –2024-R-81 A Resolution of the City Commission of the City of Holly Hill, Florida, Authorizing the City Manager to Execute Change Order No. 2 with Parker Mynchenberg & Associates, Inc., to Include Construction Administration Services for the 10Th Street Sewer Main Extension Project in an Amount Not to Exceed $6,075.00; Providing for Severability; and Providing for an Effective Date.

   (Requested by Antoine Khoury, Public Works)

3. Resolution –2024-R-82 A Resolution of the City Commission of the City of Holly Hill, Florida, Approving Price Agreements for the Purchase of the Fiscal Year 2024-2025 Supply of Water and Wastewater Treatment Chemicals for the Public Works Department and Authorize the City Manager to Execute Any Necessary Price Agreements; Providing for Severability; and Providing for an Effective Date.

(Requested by Antoine Khoury, Public Works)

4. Resolution –2024-R-83 A Resolution of the City Commission of the City of Holly Hill, Florida, Approving the Repair of the Sewer Main at 2Nd Street and Carswell Avenue by Black Sands Development, LLC, at a Cost of $110,206.90 and Authorize the City Manager to Execute the Same; Providing for Severability; and Providing for an Effective Date.

   (Requested by Antoine Khoury, Public Works)

5. Resolution –2024-R-84 A Resolution of the City of Holly Hill, Florida, Approving the Piggyback of Charlotte County Contract #2021000541, Awarding the Purchase of (4) 2024 Police Vehicles from Bartow Ford at a Cost of $211,144.11 and Authorizing the City Manager to Execute the Same; Providing for Severability; and Providing for an Effective Date.

   (Requested by Antoine Khoury, Public Works)

6. Resolution –2024-R-85 A Resolution of the City Commission of the City of Holly Hill, Florida, Establishing a "Not to Exceed" Price of $1,000,000 with Phillips & Jordan, Inc., for the Provision of Debris Hauling Services Following Hurricane Milton, Establishing a "Not to Exceed" Price of $400,000 with Tetra-Tech, Inc., for the Provision of Debris Monitoring Services Following Hurricane Milton, and Authorizing the City Manager to Execute the Same; Providing for Severability; and Providing for an Effective Date.

   (Requested by Michele Moore, Finance)

7. Resolution –2024-R-86 A Resolution of the City Commission of the City of Holly Hill, Florida, Authorizing the City Manager to Execute an Addendum to Agreement RFP 19-PW-16 with Phillips & Jordan, Inc., for Emergency Debris Hauling; Providing for Severability; and Providing for an Effective Date.

   (Requested by Valerie Manning, City Clerk)

8. Fully Insured Group Insurance and Ancillary Lines of Coverage - January 1, 2025 - December 31, 2025

   (Requested by Valerie Manning, City Clerk)

6. REGULAR AGENDA

1. Resolution –2024-R-78 A Resolution of the City of Holly Hill, Florida, Awarding the Naming Rights Of the Building Located at 1060 Ridgewood Avenue to Florida Health Care Plans, Inc., Providing for Severability; Providing for Conflicting Resolutions; And Providing for an Effective Date.

   (Requested by Joseph Forte, City Manager)

2. Resolution –2024-R-87 A Resolution of the City Commission of the City of Holly Hill, Volusia County, Florida, Providing for a Temporary Waiver of Building Permit Fees for Anticipated Repairs to Building or Structural Damage Caused by Hurricane Milton; Providing for an Intent and Purpose of This Resolution; Providing for a Filing Period for Eligible Building Permit Applications; Providing for Severability; and Providing for an Effective Date.

   (Requested by Brian Walker, Board of Planning and Appeals)

7. PUBLIC HEARINGS

Please silence any cell phone, pager or noise making device as not to interrupt the meeting. Staff will introduce each item for consideration, with comments and recommendations. The applicant or appellant and supporters will be heard first. Those in opposition to the request will be heard next. Comments should be restricted to pertinent information regarding the agenda item under discussion. Out of courtesy to others, we ask that speakers keep their comments brief and try to limit these comments to information not previously discussed. Speakers should state their name and address clearly for the record. The City Clerk's office is required to retain any documents, photographs, drawings, etc. that are shown to the City Commissioners in support of a position. The City Commission may ask questions of speakers or of staff members. The Mayor will then ask the City Commission to make a recommendation or motion. Once a motion has been made and seconded, discussion will be closed to the floor. Following City Commission discussion, a vote will be taken. During voting, Commissioners who do not cast objecting votes are considered to have voted in support of the motion.

1. Ordinance –2024-O-3079 FIRST READING - an Ordinance of the City of Holly Hill, Florida, Amending the Land Development Regulations, by Amending the Official Zoning Map to Designate the Property Described in Exhibit a from CC-1 (Commercial Corridor District) to Business Planned Unit Development (BPUD) (Business Planned Unit Development); Providing for Conflicting Ordinances; Providing for Severability; and Providing an Effective Date.

   (Requested by Brian Walker, Board of Planning and Appeals)

8. COMMUNICATIONS

A. City Manager Comments
B. City Attorney Comments
C. City Commission Comments
D. Mayor's Comments

9. FAREWELL COMMENTS

A. Mayor Chris Via
B. City Commissioner John Danio

10. ADJOURNMENT

Website Address – www.hollyhillfl.org (City Clerk)

NOTICE – If any person decides to appeal any decision of the City Commission at this meeting, he/she will need a record of the proceedings and, for that purpose, he/she may need to ensure that a verbatim record of the proceedings is made, which record includes the testimony and evidence upon which the appeal is to be based. The City does not prepare or provide such a record.



For special accommodations, please notify the City Clerk's Office at least 72 hours in advance. (386) 248-9441



Help for the hearing impaired is available through the Assistive Listening System. Receivers can be obtained from the City Clerk's Office.

In accordance with the Americans with Disabilities Act (ADA), persons needing a special accommodation to participate in the Commission proceedings should contact the City Clerk's Office no later than three (3) days prior to the proceedings.

HOLLY HILL
FLORIDA

City Commission
1065 Ridgewood Ave
Holly Hill, FL 32117

SCHEDULED

Meeting: 10/22/24 06:00 PM
Department: City Clerk
Category: Presentation
Prepared By: Valerie Manning
Initiator: Valerie Manning
Sponsors:
DOC ID: 4669

PRESENTATION (ID # 4669)

Government Finance Officers Association - Award of Excellence

BACKGROUND

Government Finance Officers Association of the United States and Canada (GFOA) has awarded the Certificate of Achievement for Excellence in Financial Reporting to City of Holly Hill for its annual comprehensive financial report for the fiscal year ended September 30, 2023. The report has been judged by an impartial panel to meet the high standards of the program, which includes demonstrating a constructive "spirit of full disclosure" to clearly communicate its financial story and motivate potential users and user groups to read the report.

The Certificate of Achievement is the highest form of recognition in the area of governmental accounting and financial reporting, and its attainment represents a significant accomplishment by a government and its management.

Government Finance Officers Association
203 North LaSalle Street, Suite 2700
Chicago, Illinois 60601-1210
312.977.9700 *fax:* 312.977.4806

10/10/2024

Joe Forte
Manager
City of Holly Hill, Florida

Dear Joe:

We are pleased to notify you that your annual comprehensive financial report for the fiscal year ended September 30, 2023 qualifies for GFOA's Certificate of Achievement for Excellence in Financial Reporting. The Certificate of Achievement is the highest form of recognition in governmental accounting and financial reporting, and its attainment represents a significant accomplishment by a government and its management.

When a Certificate of Achievement is awarded to a government, an Award of Financial Reporting Achievement (AFRA) is also presented to the individual(s) or department designated by the government as primarily responsible for its having earned the Certificate. This award has been sent to the submitter as designated on the application.

We hope that you will arrange for a formal presentation of the Certificate and Award of Financial Reporting Achievement, and give appropriate publicity to this notable achievement. A sample news release is included to assist with this effort.

We hope that your example will encourage other government officials in their efforts to achieve and maintain an appropriate standard of excellence in financial reporting.

Sincerely,

Michele Mark Levine
Director, Technical Services

Attachment: Announcement of Award (4669 : Government Finance Officers Association - Award of Excellence)



Government Finance Officers Association

Certificate of Achievement for Excellence in Financial Reporting

Presented to

City of Holly Hill
Florida

For its Annual Comprehensive
Financial Report
For the Fiscal Year Ended

September 30, 2023

Christopher P. Morrill

Executive Director/CEO

Attachment: Certificate of Achievement (4669 : Government Finance Officers Association - Award of Excellence)

STAFF REPORT
CITY OF HOLLY HILL, FLORIDA

City Commission
Agenda Item

MEETING DATE: **October 22, 2024**
FROM: **Valerie Manning**
SUBJECT: **Minutes - October 8, 2024 Regular City Commission Meeting**
NUMBER: **(ID # 4664)**
APPLICANT:
PLANNER:

DISCUSSION:

Minutes from the October 8, 2024 regular City Commission meeting.

MOTION:

Approve the minutes as submitted by staff.

- Minutes - October 8, 2024 - Regular City Commission meeting (PDF)

CITY OF HOLLY HILL, FLORIDA

CITY COMMISSION

MINUTES ● OCTOBER 8, 2024

City Commission Chamber **Regular City Commission Meeting** **6:00 PM**

CITY HALL
1065 RIDGEWOOD AVENUE
HOLLY HILL, FL 32117

City Clerk's office: (386) 248-9441 - Fax: (386) 248-9448

1. CALL TO ORDER

a. Roll Call

Attendee Name	Title	Status	Arrived
Chris Via	Mayor	Present	
John Penny	District 1 - Commissioner	Present	
Penny Currie	District 2 - Commissioner	Present	
John C. Danio	District 3 - Commissioner	Present	
Roy Johnson	District 4 - Commissioner	Present	

b. Invocation by Commissioner John Danio
Commissioner Danio led the invocation.

c. Pledge of Allegiance
Mayor Via led the Pledge of Allegiance to the Flag.

2. PUBLIC COMMENTS

None.

3. APPROVAL OF MINUTES

1. -DOC-2024-8

Minutes - September 24, 2024 Regular City Commission and Second PH on the Budget FY25 Meeting

(Requested by Valerie Manning, City Clerk)
Mayor Via opened public participation. No one spoke.

RESULT:	**APPROVED [UNANIMOUS]**
MOVER:	Roy Johnson, District 4 - Commissioner
SECONDER:	John C. Danio, District 3 - Commissioner
AYES:	Via, Penny, Currie, Danio, Johnson

Enacted and approved this 8th day of October, 2024, in Holly Hill

Attachment: Minutes - October 8, 2024 - Regular City Commission meeting (4664 : Minutes)

4. CONSENT AGENDA - ITEMS (1 - 2)

Mayor Via asked if there was anyone in the audience who wished to speak on any item on the Consent Agenda or if any member of the City Commission wished to pull an item for further discussion. There was no one.

1. –2024-R-75 Resolution

A Resolution of the City Commission of the City of Holly Hill, Florida Awarding the Contract for Sewer Extension Construction to Hazen Construction, Inc., in the Amount of $464,972.00.00 and Authorizing the City Manager to Execute the Same; Providing for Severability; and Providing for an Effective Date.

(Requested by Antoine Khoury, Public Works)

RESULT:	**ADOPTED [UNANIMOUS]**
MOVER:	John C. Danio, District 3 - Commissioner
SECONDER:	Roy Johnson, District 4 - Commissioner
AYES:	Via, Penny, Currie, Danio, Johnson

RESOLUTION
2024-R-75
A RESOLUTION OF THE CITY COMMISSION OF THE CITY OF HOLLY HILL, FLORIDA AWARDING THE CONTRACT FOR SEWER EXTENSION CONSTRUCTION TO HAZEN CONSTRUCTION, INC., IN THE AMOUNT OF $464,972.00.00 AND AUTHORIZING THE CITY MANAGER TO EXECUTE THE SAME; PROVIDING FOR SEVERABILITY; AND PROVIDING FOR AN EFFECTIVE DATE.

A RESOLUTION OF THE CITY COMMISSION OF THE CITY OF HOLLY HILL, FLORIDA AWARDING THE CONTRACT FOR SEWER EXTENSION CONSTRUCTION TO HAZEN CONSTRUCTION, INC., IN THE AMOUNT OF $464,972.00.00 AND AUTHORIZING THE CITY MANAGER TO EXECUTE THE SAME; AND PROVIDING FOR SEVERABILITY; AND PROVIDING FOR AN EFFECTIVE DATE.

WHEREAS, An Invitation to Bid was advertised for the construction of a sewer main extension along 10th Street; and

WHEREAS, Two (2) proposals were received for this project; and

WHEREAS, Hazen Construction, Inc., was the apparent low bidder for this project; and

WHEREAS, the proposal from Hazen Construction, Inc., has been vetted with a recommendation of award given by Parker Mynchenberg & Associates, Inc.; and

WHEREAS, the City Utility received a State Grant LPA0541 with Resolution Number 2023-R-26 to provide reimbursement of up to $1,360,000.00 in engineering and construction to fund this project.

Attachment: Minutes - October 8, 2024 - Regular City Commission meeting (4664 : Minutes)

NOW, THEREFORE, BE IT RESOLVED BY THE CITY COMMISSION OF THE CITY OF HOLLY HILL, FLORIDA:

SECTION 1. That the City Commission of the City of Holly Hill award the contract of construction of a sewer main extension along 10th Street to Hazen Construction, Inc., in the amount of $464,972.00.00 and authorize the City Manager to execute the same.

SECTION 2. SEVERABILITY. If any section or portion of a section of this Resolution proves to be invalid, unlawful, or unconstitutional, it shall not be held to invalidate or impair the validity, force, or effect of any other section or part of this Resolution.

SECTION 3. EFFECTIVE DATE. This Resolution shall take effect immediately upon its adoption.

APPROVED AND AUTHENTICATED on this 8th day of OCTOBER, 2024.

Enacted and approved this 8th day of October, 2024, in Holly Hill

2. –2024-R-76 Resolution

A Resolution of the City Commission of the City of Holly Hill, Florida, Approving Price Agreements for the Purchase of the Fiscal Year 2024-2025 Supply of Water and Wastewater Treatment Chemicals for the Public Works Department by Waiving Formal Bidding and Approving Piggybacking Contracts and Authorize the City Manager to Execute Any Necessary Price Agreements; Providing for Severability; and Providing for an Effective Date.

(Requested by Antoine Khoury, Public Works)

RESULT:	**ADOPTED [UNANIMOUS]**
MOVER:	John C. Danio, District 3 - Commissioner
SECONDER:	Roy Johnson, District 4 - Commissioner
AYES:	Via, Penny, Currie, Danio, Johnson

RESOLUTION
2024-R-76
A RESOLUTION OF THE CITY COMMISSION OF THE CITY OF HOLLY HILL, FLORIDA, APPROVING PRICE AGREEMENTS FOR THE PURCHASE OF THE FISCAL YEAR 2024-2025 SUPPLY OF WATER AND WASTEWATER TREATMENT CHEMICALS FOR THE PUBLIC WORKS DEPARTMENT BY WAIVING FORMAL BIDDING AND APPROVING PIGGYBACKING CONTRACTS AND AUTHORIZE THE CITY MANAGER TO EXECUTE ANY NECESSARY PRICE AGREEMENTS; PROVIDING FOR SEVERABILITY; AND PROVIDING FOR AN EFFECTIVE DATE.

A RESOLUTION OF THE CITY COMMISSION OF THE CITY OF HOLLY HILL, FLORIDA, APPROVING PRICE

Attachment: Minutes - October 8, 2024 - Regular City Commission meeting (4664 : Minutes)

AGREEMENTS FOR THE PURCHASE OF THE FISCAL YEAR 2024-2025 SUPPLY OF WATER AND WASTEWATER TREATMENT CHEMICALS FOR THE PUBLIC WORKS DEPARTMENT BY WAIVING FORMAL BIDDING AND APPROVING PIGGYBACKING CONTRACTS AND AUTHORIZE THE CITY MANAGER TO EXECUTE ANY NECESSARY PRICE AGREEMENTS; PROVIDING FOR SEVERABILITY; AND PROVIDING FOR AN EFFECTIVE DATE.

WHEREAS, the City of Holly Hill is in need of chemicals for water and wastewater treatment; and

WHEREAS, the City of Holly Hill has identified an existing, competitively bid contract for the purchase of carbon dioxide with the City of Ocala; and

WHEREAS, the City of Holly Hill has identified an existing, competitively bid contract for the purchase of high calcium quicklime with the City of Edgewater; and

WHEREAS, there are only three companies in Florida capable of providing the City with liquid chlorine and liquid sulfur dioxide and the City received price quotes from two of these companies and one company declined to provide a proposal; and

WHEREAS, Chapter 287, Florida Statutes, grants the authority to piggyback the purchase of goods and services as a form of intergovernmental cooperative purchasing in which a public purchaser requests competitive sealed bids, enters into a contract, and arranges, as part of the contract, for other public purchasing units to purchase from the selected vendor under the same terms and conditions as itself in order to take advantage of the better pricing that large purchasers are able to obtain in order to reduce administrative time and costs involved in the procurement process (i.e., cost of preparing bid specifications, advertising, etc.); and

WHEREAS, the City Commission approves the price agreements for the purchase of Fiscal Year 2024-2025 supply of water and wastewater treatment chemicals for the Public Works Department.

NOW, THEREFORE, BE IT RESOLVED BY THE CITY COMMISSION OF THE CITY OF HOLLY HILL, FLORIDA:

SECTION 1. That the City Commission does hereby approve the piggybacking of contracts for the purchase of carbon dioxide and high calcium quicklime. The City Commission also waives the formal bidding process for the purchase of liquid chlorine and liquid sulfur dioxide and awards the contract to Allied Universal Corporation. The City Commission hereby approves all price agreements for the purchase of the Fiscal Year 2024-25 supply of water and wastewater treatment chemicals for the Public Works Department and authorizes City Manager to execute any necessary price agreements.

Attachment: Minutes - October 8, 2024 - Regular City Commission meeting (4664 : Minutes)

SECTION 2. SEVERABILITY. If any section or portion of a section of this Resolution proves to be invalid, unlawful, or unconstitutional, it shall not be held to invalidate or impair the validity, force, or effect of any other section or part of this Resolution.

SECTION 3. EFFECTIVE DATE. This Resolution shall take effect immediately upon its adoption.

APPROVED AND AUTHENTICATED on this 8th day of OCTOBER, 2024.

Enacted and approved this 8th day of October, 2024, in Holly Hill

5. REGULAR AGENDA

1. –2024-R-77 Resolution

A Resolution of the City Commission of the City of Holly Hill, Florida, Approving the Position and Utilization of a Canine (K-9) Unit for the Holly Hill Police Department; Providing for Severability; and Providing for an Effective Date.

(Requested by Valerie Manning, City Clerk)
Mayor Via opened public participation. No one spoke.

RESULT:	**ADOPTED [UNANIMOUS]**
MOVER:	Penny Currie, District 2 - Commissioner
SECONDER:	John Penny, District 1 - Commissioner
AYES:	Via, Penny, Currie, Danio, Johnson

RESOLUTION
2024-R-77
A RESOLUTION OF THE CITY COMMISSION OF THE CITY OF HOLLY HILL, FLORIDA, APPROVING THE POSITION AND UTILIZATION OF A CANINE (K-9) UNIT FOR THE HOLLY HILL POLICE DEPARTMENT; PROVIDING FOR SEVERABILITY; AND PROVIDING FOR AN EFFECTIVE DATE.

A RESOLUTION OF THE CITY COMMISSION OF THE CITY OF HOLLY HILL, FLORIDA, APPROVING THE POSITION AND UTILIZATION OF A CANINE UNIT FOR THE HOLLY HILL POLICE DEPARTMENT; PROVIDING FOR SEVERABILITY; AND PROVIDING FOR AN EFFECTIVE DATE.

WHEREAS, The City of Holly Hill Police Department has identified a need for a Canine (K-9) Unit to include canine cruiser; and

Attachment: Minutes - October 8, 2024 - Regular City Commission meeting (4664 : Minutes)

WHEREAS, the primary goal of the K-9 Unit is to enhance the police department's objectives in providing quality law enforcement service to the community. Police K-9 teams are valuable tools in accomplishing law enforcement objectives of criminal apprehension and search and seizure; and

WHEREAS, the police K-9 breed will be a German Shepherd.

WHEREAS, the K-9 shall remain under the care of Sergeant Nikolas Stacy at his residence; and

WHEREAS, this is a Capital Project identified in the FY24-25 budget cycle; and

WHEREAS, the requested amount for the initial cost of the K-9 is $12,500.00 through Southern Coast K-9 Incorporated.

NOW, THEREFORE, BE IT RESOLVED BY THE CITY COMMISSION OF THE CITY OF HOLLY HILL, FLORIDA AS FOLLOWS:

SECTION 1. That the City Commission of the City of Holly Hill approve the position of K-9 Unit, to include the care, training, and maintenance of the canine and its liabilities.

SECTION 2. The City Commission directs the Police Chief to develop a plan for the implementation of the K-9 Unit, including but not limited to, the selection of qualified officers for K-9 handler roles, procurement of suitable K-9s, and acquisition of necessary equipment, facilities, and training.

SECTION 3. Funding for the K-9 Unit shall be derived from existing law enforcement budgets, grants, community donations, or other appropriate sources as deemed necessary by the City of Holly Hill.

SECTION 4. The K-9 Unit shall be utilized for purposes including, but not limited to, narcotics detection, suspect apprehension, search and rescue, and community policing initiatives.

SECTION 5. SEVERABILITY. If any section or portion of a section of this Resolution proves to be invalid, unlawful, or unconstitutional, it shall not be held to invalidate or impair the validity, force, or effect of any other section or part of this Resolution.

SECTION 6. EFFECTIVE DATE. This Resolution shall take effect immediately upon its adoption.

APPROVED AND AUTHENTICATED on this 8th day of OCTOBER, 2024.

Enacted and approved this 8th day of October, 2024, in Holly Hill

2. -2024-R-78 Resolution

Attachment: Minutes - October 8, 2024 - Regular City Commission meeting (4664 : Minutes)

A Resolution of the City of Holly Hill, Florida, Awarding the Naming Rights Of the Building Located at 1060 Ridgewood Avenue to Florida Health Care Plans, Inc., Providing for Severability; Providing for Conflicting Resolutions; And Providing for an Effective Date.

(Requested by Joseph Forte, City Manager)
Mr. Forte informed the Mayor and City Commissioners that this item will be pulled and placed on the October 22, 2024 regular City Commission meeting.

RESULT:	**PULLED BY CITY MANAGER**	**Next: 10/22/2024 6:00 PM**

3. –DOC-2024-9

Extention of Bike Week / Biketoberfest Events

(Requested by Brian Walker, Board of Planning and Appeals)
Mayor Via opened public participation. No one spoke.

RESULT:	**APPROVED [UNANIMOUS]**
MOVER:	John Penny, District 1 - Commissioner
SECONDER:	Penny Currie, District 2 - Commissioner
AYES:	Via, Penny, Currie, Danio, Johnson

Enacted and approved this 8th day of October, 2024, in Holly Hill

6. PUBLIC HEARINGS - NONE

7. COMMUNICATIONS

A. City Manager Comments
Mr. Forte introduced Amy Zengotita as the city's new Economic Development Manager/CRA Coordinator. Informed everyone about the Local State of Emergency Resolution and that was read into the record at this time.

Attorney Simpson read by title only:

RESOLUTION 2024-R-79

A RESOLUTION OF THE CITY COMMISSION OF THE CITY OF HOLLY HILL, FLORIDA, DECLARING A LOCAL STATE OF EMERGENCY; PROVIDING FOR SEVERABILITY; AND PROVIDING FOR AN EFFECTIVE DATE.

WHEREAS, **Tropical Storm Milton** is a major hurricane and is projected to impact within the corporate limits of the City of Holly Hill, Florida posing a severe threat to the health safety and wellbeing of its residents; and

Attachment: Minutes - October 8, 2024 - Regular City Commission meeting (4664 : Minutes)

WHEREAS, Governor Ron DeSantis issued Executive Order 24-215 on October 6, 2024, declaring a State of Emergency for the State of Florida with regard to Tropical Storm Milton; and

WHEREAS, under the provisions of Florida Statute 252.38(5), local subdivisions have the authority to request state assistance or invoke emergency-related Mutual Aid assistance by declaring a state of local emergency.

NOW, THEREFORE, BE IT RESOLVED BY THE CITY COMMISSION OF THE CITY OF HOLLY HILL, FLORIDA:

SECTION 1. The City Commission does hereby declare that a State of Emergency exists within the City of Holly Hill, Florida.

SECTION 2. The Holly Hill Comprehensive Emergency Management Plan shall be fully executed.

SECTION 3. The City Manager is formally directed to engage all City resources to provide such assistance as can be delivered, and to coordinate all departments to provide assistance and support for the protection of life and property, to assist and coordinate with other local, county, state and federal emergency management agencies, to order evacuations and curfews as necessary, and to take any and all emergency response actions required to safeguard life and property and ensure continuity of government services and operations within the City of Holly Hill, Florida.

SECTION 4. Under this State of Emergency, as provided in Florida Statute 252.38(5), the City Manager is hereby authorized to waive procedures and formalities otherwise required by law pertaining to:

To request state assistance or invoke emergency-related mutual-aid assistance by declaring a state of local emergency in the event of an emergency affecting only one political subdivision. The duration of each state of emergency declared locally is limited to 7 days; it may be extended, as necessary, in 7-day increments. Further, the political subdivision has the power and authority to waive the procedures and formalities otherwise required of the political subdivision by law pertaining to:

a. Performance of public work and taking whatever prudent action is necessary to ensure the health, safety, and welfare of the community.

b. Entering into contracts.

c. Incurring obligations.

d. Employment of permanent and temporary workers.

e. Utilization of volunteer workers.

f. Rental of equipment.

g. Acquisition and distribution, with or without compensation, of supplies, materials, and facilities.

Attachment: Minutes - October 8, 2024 - Regular City Commission meeting (4664 : Minutes)

h. Appropriation and expenditure of public funds.

SECTION 5. SEVERABILITY. If any section or portion of this Resolution proves to be invalid, unlawful, or unconstitutional, it shall not be held to invalidate or impair the validity, force, or effect of any other section or part of this Resolution.

SECTION 6. EFFECTIVE DATE. This Resolution shall take effect immediately upon its adoption by the City Commission, but shall expire seven (7) calendar days from the date of adoption.

The within and foregoing Resolution was read before the City Commission of the City of Holly Hill, Florida, at a regularly scheduled City Commission meeting in the Commission Chambers at 1065 Ridgewood Avenue, Holly Hill, Florida on the 8th day of October, 2024.

APPROVED AND AUTHENTICATED on this 8th day of OCTOBER, 2024.

Commissioner Johnson made a motion to ***APPROVE RESOLUTION 2024-R-79, DECLARING A LOCAL STATE OF EMERGENCY DUE TO HURRICANE MILTON,*** *seconded by Commissioner Currie.*

Mayor Via opened public participation. No one spoke.

PASSED, 5-0.

Mr. Forte reminded the Mayor and Commissioners about the two workshops coming up at the end of the month; October 23rd and October 30th.

B. City Attorney Comments
None.

C. City Commission Comments
Commissioners Penny, Currie, Danio, Johnson and Mayor Via mentioned how great National Night Out was this year and how well attended it was; they believe it was bigger than last year and it continues to grow. Thanked everyone that helped that evening and thanked Chief Williams and the Police Officers for a really great event. Commissioner Penny thanked everyone for coming to the 28th Mayor's Golf Tournament last Saturday. It was a great tournament, raised a good amount of money totaling $16,000; $8,000 for the Kiwanis Reading Summer Program for 2025 at the Holly Hill School and $8,000 for the Holly Hill Police Foundation.

Commissioner Penny made a motion to ***CANCEL THE NOVEMBER 26, 2024 REGULAR CITY COMMISSION MEETING DUE TO THE THANKSGIVING DAY HOLIDAY AND CANCEL THE DECEMBER 24, 2024 REGULAR CITY COMMISSION MEETING DUE TO THE CHRISTMAS HOLIDAY,*** *seconded by Commissioner Currie.*

Mayor Via opened public participation. No one spoke.

PASSED, 5-0.

Attachment: Minutes - October 8, 2024 - Regular City Commission meeting (4664 : Minutes)

Commissioner Johnson reminded everyone about the upcoming Car Show on Saturday, October 19th here at City Hall; TPO meeting update; Hurricane Milton mentioned.

D. Mayor's Comments

Mayor Via mentioned the flooding concerns for the city due to Hurricane Milton, encouraged everyone to be safe; thanked staff for all the hard work with the sandbag operations, posting to social media and keeping the public up to date with hurricane information; reminded everyone that there will be power outages and to be prepared for that; many of the FPL linemen are still out of the State helping to restore the people from Hurricane Helene but there are many here as well; it may take a little longer to get power restored but it will be. Debris will be picked up as quick as possible but that will be take some time as well.

8. ADJOURNMENT

The meeting adjourned at approximately 6:45 PM.

Attachment: Minutes - October 8, 2024 - Regular City Commission meeting (4664 : Minutes)

HOLLY HILL
FLORIDA

STAFF REPORT
CITY OF HOLLY HILL, FLORIDA

City Commission
Resolution

MEETING DATE: October 22, 2024
FROM: Valerie Manning
SUBJECT: A Resolution of the City Commission of the City of Holly Hill, Florida, Adopting the National Institute of Standards and Technology Cybersecurity Framework and Authorize the Chief Technology Officer to Complete the Local Governance Cybersecurity Standards Attestation Form Via the Florida Digital Service Online Portal Before January 1, 2025 Deadline; Providing for Severability; and Providing for an Effective Date.
NUMBER: 2024-R-80
APPLICANT:
PLANNER:

DISCUSSION:

Florida Statute 282.3185 (4) Cybersecurity Standards states:

- () Each local government shall adopt cybersecurity standards that safeguard its data, information technology, and information technology resources to ensure availability, confidentiality, and integrity. The cybersecurity standards must be consistent with generally accepted best practices for cybersecurity, including the National Institute of Standards and Technology Cybersecurity Framework.
- () Each county with a population of 75,000 or more must adopt the cybersecurity standards required by this subsection by January 1, 2024. Each county with a population of less than 75,000 must adopt the cybersecurity standards required by this subsection by January 1, 2025.
- () Each municipality with a population of 25,000 or more must adopt the cybersecurity standards required by this subsection by January 1, 2024. Each municipality with a population of less than 25,000 must adopt the cybersecurity standards required by this subsection by January 1, 2025.
- () Each local government shall notify the Florida Digital Service of its compliance with this subsection as soon as possible.

FISCAL ANALYSIS:

N/A

STAFF RECOMMENDATION:

Approve the adoption of the National Institute of Standards and Technology Cybersecurity Framework and authorize the Chief Technology Officer to complete the Local Governance Cybersecurity Standards Attestation Form via the Florida Digital Service online portal before the January 1, 2025, deadline to affirm that required standards have been adopted.

MOTION:

APPROVE THE ADOPTION OF THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY CYBERSECURITY FRAMEWORK AND AUTHORIZE THE CHIEF TECHNOLOGY OFFICER TO COMPLETE THE LOCAL GOVERNANCE CYBERSECURITY STANDARDS ATTESTATION FORM VIA THE FLORIDA DIGITAL SERVICE ONLINE PORTAL BEFORE THE JANUARY 1, 2025 DEADLINE TO AFFIRM THAT REQUIRED STANDARDS HAVE BEEN ADOPTED.

ATTACHMENTS:

- NIST MEP Cybersecurity Handbook (PDF)

Resolution No. 2024-80

A RESOLUTION OF THE CITY COMMISSION OF THE CITY OF HOLLY HILL, FLORIDA, ADOPTING THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY CYBERSECURITY FRAMEWORK AND AUTHORIZE THE CHIEF TECHNOLOGY OFFICER TO COMPLETE THE LOCAL GOVERNANCE CYBERSECURITY STANDARDS ATTESTATION FORM VIA THE FLORIDA DIGITAL SERVICE ONLINE PORTAL BEFORE JANUARY 1, 2025 DEADLINE; PROVIDING FOR SEVERABILITY; AND PROVIDING FOR AN EFFECTIVE DATE.

A RESOLUTION OF THE CITY COMMISSION OF THE CITY OF HOLLY HILL, FLORIDA, ADOPTING THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY CYBERSECURITY FRAMEWORK AND AUTHORIZE THE CHIEF TECHNOLOGY OFFICER TO COMPLETE THE LOCAL GOVERNANCE CYBERSECURITY STANDARDS ATTESTATION FORM VIA THE FLORIDA DIGITAL SERVICE ONLINE PORTAL BEFORE THE JANUARY 1, 2025 DEADLINE; PROVIDING FOR SEVERABILITY; AND PROVIDING FOR AN EFFECTIVE DATE.

WHEREAS, Florida Statute 282.3185(4) Cybersecurity Standards states the following:

() Each local government shall adopt cybersecurity standards that safeguard its data, information technology, and information technology resources to ensure availability, confidentiality, and integrity. The cybersecurity standards must be consistent with generally accepted best practices for cybersecurity, including the National Institute of Standards and Technology Cybersecurity Framework.

() Each county with a population of 75,000 or more must adopt the cybersecurity standards required by this subsection by January 1, 2024. Each county with a population of less than 75,000 must adopt the cybersecurity standards required by this subsection by January 1, 2025.

() Each municipality with a population of 25,000 or more must adopt the cybersecurity standards required by this subsection by January 1, 2024. Each municipality with a population of less than 25,000 must adopt the cybersecurity standards required by this subsection by January 1, 2025.

() Each local government shall notify the Florida Digital Service of its compliance with this subsection as soon as possible.

NOW, THEREFORE, BE IT RESOLVED BY THE CITY COMMISSION OF

THE CITY OF HOLLY HILL, FLORIDA:

SECTION 1. That the City Commission of the City of Holly Hill approve the adoption of the National Institute of Standards and Technology Cybersecurity Framework and authorize the Chief Technology Officer to complete the Local Governance Cybersecurity Standards Attestation Form via the Florida Digital Service online portal before the January 1, 2025, deadline to affirm that required standards have been adopted.

SECTION 2. SEVERABILITY. If any section or portion of a section of this Resolution proves to be invalid, unlawful, or unconstitutional, it shall not be held to invalidate or impair the validity, force, or effect of any other section or part of this Resolution.

SECTION 3. EFFECTIVE DATE. This Resolution shall take effect immediately upon its adoption.

APPROVED AND AUTHENTICATED on this 22nd day of OCTOBER, 2024.

NIST Handbook 162

NIST MEP Cybersecurity Self-Assessment Handbook For Assessing NIST SP 800-171 Security Requirements in Response to DFARS Cybersecurity Requirements

Patricia Toth

This publication is available free of charge from:
https://doi.org/10.6028/NIST.HB.162

National Institute of Standards and Technology
U.S. Department of Commerce

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

NIST Handbook 162

NIST MEP Cybersecurity Self-Assessment Handbook For Assessing NIST SP 800-171 Security Requirements in Response to DFARS Cybersecurity Requirements

Patricia Toth
Programs and Partnerships Division
Manufacturing Extension Partnership

This publication is available free of charge from:
https://doi.org/10.6028/NIST.HB.162

November 2017



U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Undersecretary of Commerce for Standards and Technology

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

Abstract

The Handbook is intended to be a guide to assist U.S. manufacturers who supply products within supply chains for the DOD and who must ensure adequate security by implementing NIST SP 800-171 as part of the process for ensuring compliance with DFARS clause 252.204-7012, “Safeguarding Covered Defense Information and Cyber Incident Reporting,” available at http://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm#252.204-7012.

Key words

assessment; compliance; Controlled Unclassified Information; CUI; cybersecurity; DFARS; DOD supply chain; information security; manufacturing; MEP; small manufacturer; self-assessment; SP 800-171.

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

Table of Contents

Disclaimer ..... **viii**
Acknowledgements ..... **viii**
About NIST MEP and the MEP National Network™ ..... **viii**
Introduction **1**
Role of NIST in SP 800-171 1
What is NIST SP 800-171 and how does a manufacturer implement it? 2
Using this Handbook to Conduct an Assessment **4**
Preparation 4
Assessment Results 6
Self-Assessment Handbook **7**
Access Control: SP 800-171 Security Family 3.1 7
3.1.1 Limit system access to authorized users, processes acting on behalf of authorized users, or devices (including other systems). 8
3.1.2 Limit system access to the types of transactions and functions that authorized users are permitted to execute. 9
3.1.3 Control the flow of CUI in accordance with approved authorizations. 10
3.1.4 Separate the duties of individuals to reduce the risk of malevolent activity without collusion. 11
3.1.5 Employ the principle of least privilege, including for specific security functions and privileged accounts. 12
3.1.6 Use non-privileged accounts or roles when accessing non-security functions. 13
3.1.7 Prevent non-privileged users from executing privileged functions and audit the execution of such functions. 14
3.1.8 Limit unsuccessful logon attempts. 15
3.1.9 Provide privacy and security notices consistent with applicable CUI rules. 16
3.1.10 Use session lock with pattern-hiding displays to prevent access/viewing of data after period of inactivity. 17
3.1.11 Terminate (automatically) a user session after a defined condition 18
3.1.12 Monitor and control remote access sessions. 19
3.1.13 Employ cryptographic mechanisms to protect the confidentiality of remote access sessions. 20
3.1.14 Route remote access via managed access control points 21
3.1.15 Authorize remote execution of privileged commands and remote access to security-relevant information. 22
3.1.16 Authorize wireless access prior to allowing such connections. 23

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.1.17 Protect wireless access using authentication and encryption..... 24
3.1.18 Control connection of mobile devices..... 25
3.1.19 Encrypt CUI on mobile devices. 26
3.1.20 Verify and control/limit connections to and use of external information systems.27
3.1.21 Limit use of organization portable storage devices on external information systems. 28
3.1.22 Control CUI posted or processed on publicly accessible information systems. ... 29
Awareness and Training: SP 800-171 Security Family 3.2 30
3.2.1 Ensure that managers, systems administrators, and users of organization information systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of organization information systems. 31
3.2.2 Ensure that organization personnel are adequately trained to carry out their assigned information security-related duties and responsibilities..... 32
3.2.3 Provide security awareness training on recognizing and reporting potential indicators of insider threat. 33
Audit and Accountability: SP 800-171 Security Family 3.3..... 34
3.3.1 Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity. 35
3.3.2 Ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions..... 36
3.3.3 Review and update audited events..... 37
3.3.4 Alert in the event of an audit process failure..... 38
3.3.5 Correlate audit review, analysis, and reporting processes for investigation and response to indications of inappropriate, suspicious, or unusual activity. 39
3.3.6 Provide audit reduction and report generation to support on-demand analysis and reporting..... 40
3.3.7 Provide an information system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records..... 41
3.3.8 Protect audit information and audit tools from unauthorized access, modification, and deletion. 42
3.3.9 Limit management of audit functionality to a subset of privileged users..... 43
Configuration Management: SP 800-171 Security Family 3.4 44
3.4.1 Establish and maintain baseline configurations and inventories of organization information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles. 45

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.4.2 Establish and enforce security configuration settings for information technology products employed in organization information systems. 47
3.4.3 Track, review, approve/disapprove, and audit changes to information systems... 48
3.4.4 Analyze the security impact of changes prior to implementation. 49
3.4.5 Define, document, approve, and enforce physical and logical access restrictions associated with changes to the information system..... 50
3.4.6 Employ the principle of least functionality by configuring the information system to provide only essential capabilities. 51
3.4.7 Restrict, disable, and prevent the use of nonessential programs, functions, ports, protocols, and services. 52
3.4.8 Apply deny-by-exception (blacklist) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting policy to allow the execution of authorized software. 53
3.4.9 Control and monitor user-installed software. 55
Identification and Authentication: SP 800-171 Security Family 3.5 56
3.5.1 Identify information system users, processes acting on behalf of users, or devices.57
3.5.2 Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to company information systems. 58
3.5.3 Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts..... 59
3.5.4 Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts..... 61
3.5.5 Prevent reuse of identifiers for a defined period. 62
3.5.6 Disable identifiers after a defined period of inactivity. 63
3.5.7 Enforce a minimum password complexity and change of characters when new passwords are created. 64
3.5.8 Prohibit password reuse for a specified number of generations. 65
3.5.9 Allow temporary password use for system logons with an immediate change to a permanent password..... 66
3.5.10 Store and transmit only encrypted representation of passwords. 67
3.5.11 Obscure feedback of authentication information. 68
Incident Response: SP 800-171 Security Family 3.6 69
3.6.1 Establish an operational incident-handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities. 70
3.6.2 Track, document, and report incidents to appropriate officials and/or authorities both internal and external to the organization..... 71
3.6.3 Test the organization incident response capability. 73

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

Maintenance: SP 800-171 Security Family 3.7 74
3.7.1 Perform maintenance on organization information systems. 75
3.7.2 Provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance. 76
3.7.3 Ensure equipment removed for off-site maintenance is sanitized of any CUI. 77
3.7.4 Check media containing diagnostics and test programs for malicious code before the media are used in the information system. 78
3.7.5 Require multifactor authentication to establish non-local maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete..... 79
3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization. 80
Media Protection: SP 800-171 Security Family 3.8..... 81
3.8.1 Protect (i.e., physically control and securely store) information system media containing CUI, both paper and digital. 82
3.8.2 Limit access to CUI on information system media to authorized users. 83
3.8.3 Sanitize or destroy information system media containing CUI before disposal or release for reuse. 84
3.8.4 Mark media with necessary CUI markings and distribution limitations. 85
3.8.5 Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas..... 86
3.8.6 Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards. 87
3.8.7 Control the use of removable media on information system components..... 88
3.8.8 Prohibit the use of portable storage devices when such devices have no identifiable owner. 89
3.8.9 Protect the confidentiality of backup CUI at storage locations. 90
Personnel Security: SP 800-171 Security Family 3.9 91
3.9.1 Screen individuals prior to authorizing access to information systems containing CUI. 92
3.9.2 Ensure that CUI and information systems containing CUI are protected during and after personnel actions such as terminations and transfers..... 93
Physical Protection: SP 800-171 Security Family 3.10 94
3.10.1 Limit physical access to company information systems, equipment, and the respective operating environments to authorized individuals..... 95
3.10.2 Protect and monitor the physical facility and support infrastructure for those information systems. 96

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.10.3 Escort visitors and monitor visitor activity. 97
3.10.4 Maintain audit logs of physical access. 98
3.10.5 Control and manage physical access devices. 99
3.10.6 Enforce safeguarding measures for CUI at alternate work sites (e.g., telework sites). 100
Risk Assessment: SP 800-171 Security Family 3.11 101
3.11.1 Periodically assess the risk to company operations (including mission, functions, image, or reputation), company assets, and individuals, resulting from the operation of company information systems and the associated processing, storage, or transmission of CUI. 102
3.11.2 Scan for vulnerabilities in the information system and applications periodically and when new vulnerabilities affecting the system are identified. 103
3.11.3 Remediate vulnerabilities in accordance with assessments of risk. 105
Security Assessment: SP 800-171 Security Family 3.12 106
3.12.1 Periodically assess the security controls in company information systems to determine if the controls are effective in their application. 107
3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in company information systems. 109
3.12.3 Monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls. 110
3.12.4 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems. 112
Systems and Communications Protection: SP 800-171 Security Family 3.13 114
3.13.1 Monitor, control, and protect company communications (i.e., information transmitted or received by organization information systems) at the external boundaries and key internal boundaries of the information systems. 115
3.13.2 Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within company information systems. 116
3.13.3 Separate user functionality from information system management functionality. 118
3.13.4 Prevent unauthorized and unintended information transfer via shared system resources. 119
3.13.5 Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks. 120
3.13.6 Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception). 121

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.13.7 Prevent remote devices from simultaneously establishing non-remote connections with the information system and communicating via some other connection to resources in external networks. 122

3.13.8 Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards. 123

3.13.9 Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity. 125

3.13.10 Establish and manage cryptographic keys for cryptography employed in the organization systems. 126

3.13.11 Employ FIPS-validated cryptography when used to protect the confidentiality of CUI. 127

3.13.12 Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device. 128

3.13.13 Control and monitor the use of mobile code. 129

3.13.14 Control and monitor the use of Voice over Internet Protocol (VoIP) technologies. 130

3.13.15 Protect the authenticity of communications sessions. 131

3.13.16 Protect the confidentiality of CUI at rest. 132

System and Information Integrity: SP 800-171 Security Family 3.14 133

3.14.1 Identify, report, and correct information and information system flaws in a timely manner. 134

3.14.2 Provide protection from malicious code at appropriate locations within organization information systems. 136

3.14.3 Monitor information system security alerts and advisories and take appropriate actions in response. 138

3.14.4 Update malicious code protection mechanisms when new releases are available. 140

3.14.5 Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed. 142

3.14.6 Monitor the information system including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks. 143

3.14.7 Identify unauthorized use of the information system. 144

Glossary 145

Appendix A: Useful Plans, Policies and Procedures 157

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

Disclaimer

The contents of this Handbook are offered as guidance only. NIST and NIST MEP do not make any warranty or representation, expressed or implied, with respect to the accuracy, completeness, or usefulness of the information contained in this Handbook, or that the use of any information, methods, or processes described in this Handbook may not infringe on privately owned rights; or assume any liabilities with respect to the use of, or for damages resulting from the use of, any information, method, or process described in this Handbook. The Handbook does not reflect official views or policy of NIST. Mention of trade names or commercial products does not constitute endorsement by or recommendation of use by NIST.

This Handbook has been produced by NIST MEP technical staff and has been reviewed by technical staff within the NIST Information Technology Laboratory. The Handbook is intended to be a guide to assist U.S. manufacturers who supply products within supply chains for the Department of Defense (DOD) and who must ensure adequate security by implementing NIST SP 800-171 as part of the process for ensuring compliance with the Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.204-7012, "Safeguarding Covered Defense Information and Cyber Incident Reporting," available at http://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm#252.204-7012.

This Handbook includes mention of official DOD policies and regulations that are part of the aforementioned DFARS clause. Such mention is public domain information and does not constitute any policy statements or regulatory enforcement by NIST. NIST is a non-regulatory agency of the U.S. Department of Commerce; as such, NIST makes no claims that use of this Handbook will satisfy the regulatory requirements of DOD in conjunction with DFARS. Compliance with the DFARS can only be satisfied through approval by the DOD in conjunction with official DFARS requirements. All matters relating to the DFARS should be directed to the DOD in conjunction with the requirements of DFARS clause 252.204-7012. Additional information about the DFARS can be obtained at http://www.acq.osd.mil/dpap/pdi/docs/ControlledTechnicalInformation_FAQ.pdf.

Acknowledgements

The author gratefully acknowledges and appreciates the thoughtful comments from NIST MEP staff members David Stieren, Brian Lagas, Marlon Walker, and Kathleen Martin, which greatly improved the overall quality and usefulness of this Handbook. Additionally, Ron Ross and Kelley Dempsey from the NIST Information Technology Laboratory's Computer Security Division provided technical guidance on the implementation of SP 800-171. Useful feedback was also received from several staff members within the DOD Office of the Chief Information Officer to ensure consistency with DFARS provisions.

About NIST MEP and the MEP National Network™

Since 1988, the National Institute of Standards and Technology (NIST) Manufacturing Extension Partnership (MEP) has been committed to strengthening U.S. manufacturing. The MEP National Network comprises 51 MEP Centers located in all 50 states and Puerto Rico, and 1,300 trusted advisors and experts at nearly 600 MEP service locations, providing any U.S. manufacturer with access to resources they need to succeed. In 2016, the MEP National Network connected with

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

25,445 manufacturers, leading to $9.3 billion in sales, $1.4 billion in cost savings, $3.5 billion in new client investments, and helping to create and retain more than 86,602 U.S. manufacturing jobs.

Supply Chain, Defense, and Cybersecurity Focus

MEP provides hands-on technical and business assistance supporting the development and competitiveness of manufacturing supply chains, including those that serve the needs of our Nation's defense industries. MEP supports U.S. manufacturers with many different aspects of supply chain management and development, including implementing strategies within the walls of a company, to engaging with suppliers and customers around the Nation and the world. Recently, MEP has been active in providing awareness and assistance to help U.S. manufacturers protect their information assets from the risks of cyberattacks. MEP serves as a national resource to help U.S. manufacturers, who supply to the DOD, implement adequate security to safeguard covered defense information that they store, process, or transmit.

Since 2013, MEP Centers have completed 2,567 projects and worked with 1,658 companies that are prime suppliers to the DOD. MEP also works with large OEM-type suppliers and their supply chains to the DOD. From 2013 to 2016, MEP worked with 706 companies that have defense industry NAICS classifications.

For additional information, visit the NIST MEP webpage at https://www.nist.gov/mep.

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

Introduction

This Self-Assessment Handbook for Assessing NIST SP 800-171 Security Requirements in response to DFARS Cybersecurity Requirements provides guidance on implementing NIST SP 800-171 in response to the Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.204-7012 “Safeguarding Covered Defense Information and Cyber Incident Reporting.”

This Handbook provides a step-by-step guide to assessing a small manufacturer’s information systems against the security requirements in NIST SP 800-171 rev 1, “Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations,” available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf.

This Handbook may also be useful for other communities interested in applying the NIST SP 800-171 security requirements, including those seeking to comply with the CUI Federal Acquisition Regulation (FAR) clause.

Role of NIST in SP 800-171

Executive Order 13556, Controlled Unclassified Information, November 4, 2010, establishes that the Controlled Unclassified Information (CUI) Executive Agent, designated as the National Archives and Records Administration (NARA), shall develop and issue such directives as are necessary to implement the CUI Program. Consistent with this tasking and with the CUI Program’s mission to establish uniform policies and practices across the federal government, NARA issued a final federal regulation in 2016 that established the required controls and markings for CUI governmentwide. This federal regulation binds agencies throughout the executive branch to uniformly apply the standard safeguards, markings, dissemination, and decontrol requirements established by the CUI Program.

In addition to defining safeguarding requirements for CUI within the federal government, NARA took to alleviate the potential impact of such requirements on nonfederal organizations by jointly developing with NIST and DOD, NIST Special Publication 800-171, and defining security requirements for protecting CUI in nonfederal systems and organizations. This approach was intended to help nonfederal entities, including contractors, to comply with the security requirements using the systems and practices they already have in place, rather than trying to use government-specific approaches. It also provides a standardized and uniform set of requirements for all CUI security needs, tailored to nonfederal systems, allowing nonfederal organizations to be in compliance with statutory and regulatory requirements, and to consistently implement safeguards for the protection of CUI. Finally, NARA, in its capacity as the CUI Executive Agent, sponsored in 2017, a single Federal Acquisition Regulation (FAR) clause that will apply the requirements contained in the federal CUI regulation and Special Publication 800-171 to contractors. This will further promote standardization to benefit a substantial number of nonfederal organizations that are attempting to meet the current range and type of contract clauses, where differing requirements and conflicting guidance from federal agencies for the same information gives rise to confusion and inefficiencies. The CUI FAR clause will also address verification and compliance requirements for the security requirements in NIST Special Publication 800-171. Until the formal process of establishing such a FAR clause takes place, the requirements in NIST Special Publication 800-171 may be

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

referenced in federal contracts consistent with federal law and regulatory requirements. If necessary, Special Publication 800-171 will be updated to remain consistent with the federal CUI regulation and the FAR clause.

What is NIST SP 800-171 and how does a manufacturer implement it?

NIST Special Publication 800-171 was developed by NIST to further its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. 3541 et seq., Public Law (P.L.) 113-283. The publication is entitled "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations," NIST SP 800-171 Revision 1, available at

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf.

NIST SP 800-171 provides federal agencies with recommended requirements for protecting the confidentiality of controlled unclassified information (CUI):

1. when the CUI is resident in nonfederal information systems and organizations;
2. when the information systems where the CUI resides are not used or operated by contractors of federal agencies or other organizations on behalf of those agencies; and
3. where there are no specific safeguarding requirements for protecting the confidentiality of CUI prescribed by the authorizing law, regulation, or governmentwide policy for the CUI category or subcategory listed in the CUI Registry.

NIST SP 800-171 requirements apply to all components of nonfederal information systems and organizations that process, store, or transmit CUI, or provide security protection for such components. A nonfederal information system is a system that does not meet the criteria for a federal system. A federal system is an information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.

The CUI requirements are intended for use by federal agencies in contractual vehicles or other agreements established between those agencies and nonfederal organizations. This includes the DOD and is resident within DFARS clauses that apply to defense contracts.

For ease of use, the NIST SP 800-171 security requirements are organized into 14 families. This Self-Assessment Handbook is organized based on these 14 families.

For each family, a brief overview is provided. Table 1 below lists the security requirement families addressed in this Handbook.

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

FAMILY	FAMILY
Access Control	Media Protection
Awareness and Training	Personnel Security
Audit and Accountability	Physical Protection
Configuration Management	Risk Assessment
Identification and Authentication	Security Assessment
Incident Response	Systems and Communications Protection
Maintenance	System and Information Integrity

Table 1. NIST SP 800-171 Security Requirement Families

The security requirement with the original numbering scheme from 800-171 is listed throughout this Handbook.

NIST SP 800-171 assumes that small manufacturers currently have IT infrastructures in place, and it is not necessary to develop or acquire new systems to handle CUI. Most small manufacturers have security measures to protect their information which may also satisfy the 800-171 security requirements. A variety of potential security solutions can be implemented to satisfy the security requirements. There is no single security solution, each small manufacturer will need to understand their operating environment and apply the security requirements to meet their situation. Small manufacturers may not have the necessary organizational structure or resources to satisfy every security requirement. It is perfectly acceptable to implement alternative, but equally effective, security measures to satisfy a security requirement.

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

Using this Handbook to Conduct an Assessment

Preparation

This Handbook is intended for use by a small manufacturer. It is expected that the business owner, chief operating officer, IT manager, security manager, and plant manager(s) will work together to assess the security of the system(s) that process, store, or transmit CUI.

Conducting security control assessments can be challenging, and resource-intensive. Successful assessments require cooperation throughout the company. Establishing expectations before, during, and after an assessment is important to achieve an acceptable outcome. Thorough preparation is an important aspect of conducting effective security control assessments.

Preparatory activities address issues relating to the cost, schedule, and performance of the assessment. Preparing for a security control assessment includes:

- ensuring that security policies are in place and understood by company employees. A list of plans and polices companies should have in place is included in Appendix A;
- establishing the objective and scope of assessments;
- notifying key employees of assessment activities and allocating resources to carry out the assessments;
- establishing communication channels among employees having an interest in the assessments;
- establishing time frames for completing the assessments;
- selecting the assessors/assessment teams that will be responsible for conducting the assessments; and
- collecting materials to provide to the assessors/assessment teams. (This may include policies, procedures, plans, specifications, designs, records, administrator/operator manuals, information system documentation, interconnection agreements, previous assessment results, and legal requirements.)

Security control assessors/assessment teams begin the assessment by:

- gaining an understanding of the company's operations (including mission, functions, and business processes) and how the information system supports those organizational operations;
- obtaining an understanding of the structure of the information system (i.e., system architecture) being assessed;
- identifying company personnel responsible for the development and implementation of the security requirements;
- meeting with company personnel to ensure understanding for assessment objectives,

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

rigor, and scope of the assessment;

- obtaining materials needed for the assessment (e.g., policies, procedures, plans, specifications, designs, records, administrator and operator manuals, information system documentation, interconnection agreements, previous assessment results);
- establishing company points of contact needed to carry out the assessments;
- obtaining previous assessment results that may be reused (e.g., audits, vulnerability scans, physical security inspections, prior security assessments, developmental testing and evaluation, vendor flaw remediation activities); and
- developing an assessment plan

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

Assessment Results

For each security requirement question that the company answers **Yes**, a statement should be included in the Security Assessment Report and System Security Plan which explains how the information system implements the requirement.

For each security requirement question that the company answers **No**, a statement should be included in the Security Assessment Report which explains why the security requirement is not met. A statement should also be included in the Plan of Action which fully describes how the unimplemented security requirements will be met, how any planned improvements will be implemented, and when the improvements will occur.

For each security requirement questions that the company answers **Partially**, a statement should be included in the Security Assessment Report which explains why the security requirement is partially met. A statement should also be included in the Plan of Action which fully describes how the partially met security requirements will be fully met, how any planned improvements will be implemented and when the improvements will occur.

For each security requirement question that the company answers **Does Not Apply**, a statement should be included in the Security Assessment Report which explains why the security requirement does not apply to your operational environment.

For each security requirement question that the company answers **Alternative Approach**, a statement should be included in the Security Assessment Report and in the System Security Plan which fully describes the alternative approach and how it is equally effective. A statement should also be included that explains how the information system implements the requirement.

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

Access Control: SP 800-171 Security Family 3.1

Access is the ability to make use of any system resource. Access control is the process of granting or denying requests to:

- use information,
- use information processing services, and
- enter company facilities.

System-based access controls are called logical access controls. Logical access controls prescribe not only who or what (in the case of a process) is permitted to have access to a system resource, but also the type of access that is permitted. These controls may be built into the operating system, incorporated into applications programs or major utilities (e.g., database management systems, communications systems), or implemented through add-on security packages. Logical access controls may be implemented internally to the system being protected or in external devices. Examples of access control security requirements include account management, separation of duties, least privilege, session lock, information flow enforcement, and session termination.

Companies should limit:

- system access to authorized users,
- processes acting on behalf of authorized users,
- devices, including other systems, and
- the types of transactions and functions that authorized users are permitted to exercise.

The requirements for using – and prohibitions against the use of – various system resources can vary from one system to another. For example, some information must be accessible to all users, some may be needed by several groups or departments, and some may only be accessed by a few individuals within the company. While users must have access to specific information needed to perform their jobs, denial of access to non-job-related information may be required. It may also be important to control the kind of access that is permitted (e.g., the ability for the average user to execute, but not change, system programs). These types of access restrictions enforce policy and help ensure that unauthorized actions are not taken.

Controlling physical access to company facilities is also important. It provides for the protection of employees, plant equipment, hardware, software, networks, and data from physical actions and events that could cause serious loss or damage to the company. This includes burglary, theft, vandalism, and terrorism.

The following security requirements fall under the Access Control family.

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.1.1 Limit system access to authorized users, processes acting on behalf of authorized users, or devices (including other systems).

Does the company use passwords?

Yes No Partially Does Not Apply Alternative Approach

Does the company have an authentication mechanism?

Yes No Partially Does Not Apply Alternative Approach

Does the company require users to logon to gain access?

Yes No Partially Does Not Apply Alternative Approach

Are account requests authorized before system access is granted?

Yes No Partially Does Not Apply Alternative Approach

Does the company maintain a list of authorized users, defining their identity and role and sync with system, application, and data layers?

Yes No Partially Does Not Apply Alternative Approach

Additional information:

User access security refers to the set of procedures by which authorized users access the system and unauthorized users are prevented accessing the system.

Where to Look:

- access control policy
- account management procedures
- access enforcement procedures
- security plan
- configuration management plan
- information system design documentation
- information system configuration settings and associated documentation
- list of active system accounts along with the name of the individual associated with each account
- list of conditions for group and role membership
- notifications or records of recently transferred, separated, or terminated employees
- list of recently disabled information system accounts along with the name of the individual associated with each account
- list of approved authorizations (user privileges)
- access authorization records
- account management compliance reviews
- information system monitoring records
- information system audit records
- remote access implementation and usage (including restrictions) procedures
- remote access authorizations

Who to Talk to:

- employees with account management responsibilities
- system/network administrators
- employees with responsibilities for managing remote access connections
- employees with information security responsibilities
- employees with access enforcement responsibilities
- system developers

Perform Test On:

- processes account management on the information system
- automated mechanisms for implementing account management
- automated mechanisms implementing access control policy
- remote access management capability

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.1.2 Limit system access to the types of transactions and functions that authorized users are permitted to execute.

Do you use access control lists to limit access to applications and data based on role and/or identity?

Yes No Partially Does Not Apply Alternative Approach

Does the system allow for the separation of access control rights and enforcement of those rights?

Yes No Partially Does Not Apply Alternative Approach

Additional information:

Even authorized users are restricted to those parts of the system that they are explicitly permitted to use. This is based on their "need-to-know" and their role within the company.

Where to Look:

- access control policy
- account management procedures
- access enforcement procedures
- security plan
- configuration management plan
- information system design documentation
- information system configuration settings and associated documentation
- list of active system accounts along with the name of the individual associated with each account
- list of conditions for group and role membership notifications or records of recently transferred, separated, or terminated employees
- list of recently disabled information system
- accounts along with the name of the individual associated with each account
- list of approved authorizations (user privileges)
- access authorization records
- account management compliance reviews
- information system monitoring records
- information system audit records
- procedures addressing remote access implementation and usage (including restrictions)
- remote access authorizations

Who to Talk to:

- personnel with account management responsibilities
- system/network administrators
- personnel with responsibilities for managing remote access connections
- personnel with information security responsibilities
- personnel with access enforcement responsibilities
- system developers

Perform Test On:

- processes account management on the information system
- automated mechanisms for implementing account management
- automated mechanisms implementing access control policy
- remote access management capability for the information system

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.1.3 Control the flow of CUI in accordance with approved authorizations.

Do you have architectural solutions to control the flow of system data?

Yes No Partially Does Not Apply Alternative Approach

Do you document information flow control enforcement by using protected processing level (e.g., defensive architecture) as a basis for flow control decisions?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

The solutions may include firewalls, proxies, encryption, and other security technologies. Information flow control regulates where information can travel within an information system and between information systems (as opposed to who is allowed to access the information) without explicit regard to subsequent accesses to that information.

Examples of flow control restrictions include:

- keeping export-controlled information from being transmitted in the clear to the internet,
- blocking outside traffic that claims to be from within the organization,
- restricting web requests to the internet that are not from the internal web proxy server, and
- limiting information transfers between organizations based on data structures and content.

Transferring information between information systems representing different security domains with different security policies introduces risk that such transfers violate one or more domain security policies. In such situations, information owners/stewards provide guidance at designated policy enforcement points between interconnected systems. The company may consider mandating specific architectural solutions when required to enforce specific security policies. Enforcement includes, for example:

- prohibiting information transfers between interconnected systems (i.e., allowing access only),
- employing hardware mechanisms to enforce one-way information flows, and
- implementing trustworthy regrading mechanisms to reassign security attributes and security label.

Companies commonly employ information flow control policies and enforcement mechanisms to control the flow of information between designated sources and destinations (e.g., networks, individuals, and devices) within information systems and between interconnected systems. Flow control is based on the characteristics of the information and/or the information path. Enforcement occurs, for example, in boundary protection devices (e.g., gateways, routers, guards, encrypted tunnels, firewalls) that employ rule sets or establish configuration settings that restrict information system services, provide a packet-filtering capability based on header information, or message filtering capability based on message content (e.g., implementing key word searches or using document characteristics). Companies may also consider the trustworthiness of filtering/ inspection mechanisms (i.e., hardware, firmware, and software components) that are critical to information flow enforcement.

Where to Look:

- access control policy
- information flow control policies
- procedures addressing information flow enforcement
- information system design documentation
- information system configuration settings and associated documentation
- information system baseline configuration
- list of information flow authorizations information system audit records
- other relevant documents or records

Who to Talk to:

- system/network administrators
- employees with information security responsibilities
- system developers

Perform Test On:

- automated mechanisms implementing information flow enforcement policy

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.1.4 Separate the duties of individuals to reduce the risk of malevolent activity without collusion.

If a user accesses data as well as maintains the system in some way, do you create separate accounts with appropriate access levels to separate functions?

Yes No Partially Does Not Apply Alternative Approach

Is there a division of responsibilities and separation of duties of individuals to eliminate conflicts of interest?

Yes No Partially Does Not Apply Alternative Approach

Additional Information:

Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. Separations of duties includes:

- Dividing mission functions and information support functions among different individuals and/or roles,
- Conducting information system support functions with different individuals (systems management, programming, configuration management, quality assurance and testing, and network security), and
- Ensuring security personnel administering access control functions do not also administer audit functions.

Where to Look:

- access control policy
- procedures addressing divisions of responsibility and separation of duties
- information system configuration settings and associated documentation
- list of divisions of responsibility and separation of duties
- information system access authorizations
- information system audit records
- other relevant documents or records

Who to Talk to:

- employees with responsibilities for defining appropriate divisions of responsibility and separation of duties
- employees with information security responsibilities
- system/network administrators

Perform Test On:

- automated mechanisms implementing separation of duties policy

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.1.5 Employ the principle of least privilege, including for specific security functions and privileged accounts.

Do you only grant enough privileges to users to allow them to do their job?

Yes No Partially Does Not Apply Alternative Approach

Does the company restrict access to privileged functions and security information to authorized employees?

Yes No Partially Does Not Apply Alternative Approach

Additional information:

The principle of least privilege requires that every process, user, or program can only access the information and resources that are needed for its valid purpose. The principle of least privilege means giving a process, program, or user account only those privileges that are essential for it to perform its intended function.

When applied to users, the term least-privileged user account (LUA) is also used. Meaning all user accounts should always run with as few privileges as possible, and launch applications with as few privileges as possible.

Where to Look:

- access control policy
- procedures addressing least privilege
- list of assigned access authorizations (user privileges)
- list of system generated privileged accounts
- list of system administration personnel
- information system configuration settings and associated documentation
- list of security functions (deployed in hardware, software, and firmware) and security-relevant information for which access must be explicitly authorized
- information system audit records
- other relevant documents or records

Who to Talk to:

- employees with responsibilities for defining least privileges necessary to accomplish specified tasks
- employees with information security responsibilities
- system/network administrators

Perform Test On:

- automated mechanisms implementing least privilege functions

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.1.6 Use non-privileged accounts or roles when accessing non-security functions.

Do users with multiple accounts (privileged and non-privileged) typically logon with the least privileged account when not performing privileged functions?

Yes No Partially Does Not Apply Alternative Approach

Can this be described or demonstrated?

Yes No Partially Does Not Apply Alternative Approach

Are users with privileged access required to use non-privileged accounts when accessing other system functions?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

This requirement limits exposure when operating from within privileged accounts or roles. The inclusion of roles addresses situations where companies implement access control policies such as role-based access control and where a change of role provides the same degree of assurance in the change of access authorizations for both the user and all processes acting on behalf of the user as would be provided by a change between a privileged and non-privileged account.

Note that the privileged account should not be used to do non-privileged functions.

NIST SP 800-171 defines a "privileged user" as "a user that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform." For example, if users' computer accounts are "administrator accounts" or have "limited administrative rights" only on their computers, are they considered a "privileged account" requiring audit for privileged functions? Since, in this case, the "ordinary users" are authorized to perform the function, they are not considered privileged users.

Where to Look:

- access control policy
- procedures addressing least privilege
- list of system generated security functions or security-relevant information assigned to information system accounts or roles
- information system configuration settings and associated documentation
- information system audit records other relevant documents or records

Who to Talk to:

- employees with responsibilities for defining least privileges necessary to accomplish specified tasks
- employees with information security responsibilities
- system/network administrators

Perform Test On:

- automated mechanisms implementing least privilege functions

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.1.7 Prevent non-privileged users from executing privileged functions and audit the execution of such functions.

Do you enable auditing of all privileged functions?

Yes No Partially Does Not Apply Alternative Approach

Do you prevent the execution of privileged functions by non-privileged users?

Yes No Partially Does Not Apply Alternative Approach

Do you control access using access control lists based on the identity or role of the user?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

NIST SP 800-171 defines a "privileged user" as "a user that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform." For example, if users' computer accounts are "administrator accounts" or have 'limited administrative rights" only on their computers, they are not considered a "privileged account" requiring audit for privileged functions. Since, in this case, the "ordinary users" are authorized to perform the function, they are not considered privileged users.

Where to Look:

- access control policy
- procedures addressing least privilege
- information system design documentation
- information system configuration settings and associated documentation
- list of privileged functions to be audited
- list of privileged functions and associated user account assignments
- list of audited events
- information system audit records
- other relevant documents or records

Who to Talk to:

- employees with responsibilities for reviewing least privileges necessary to accomplish specified tasks
- employees with responsibilities for defining least privileges necessary to accomplish specified tasks
- employees with information security responsibilities
- system/network administrators
- system developers

Perform Test On:

- automated mechanisms auditing the execution of least privilege functions
- automated mechanisms implementing least privilege functions for non-privileged users

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.1.8 Limit unsuccessful logon attempts.

Is the system configured to limit the number of invalid logon attempts?

Yes No Partially Does Not Apply Alternative Approach

Is the system configured to lock the logon mechanism for a predetermined time after a predetermined number of invalid logon attempts?

Yes No Partially Does Not Apply Alternative Approach

Is the system configured to lock users out after a predetermined number of invalid logon attempts?

Yes No Partially Does Not Apply Alternative Approach

Does the system enforce a limit of a defined number of consecutive invalid access attempts during a defined time?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

This requirement seeks to limit the number of logon attempts. Multiple unsuccessful logon attempts may indicate malicious attacks on the information system.

Where to Look:

- access control policy
- procedures addressing unsuccessful logon attempts
- security plan
- information system design documentation
- information system configuration settings and associated documentation information system audit records
- other relevant documents or records

Who to Talk to:

- employees with information security responsibilities
- system developers
- system/network administrators

Perform Test On:

- automated mechanisms implementing access control policy for unsuccessful logon attempts

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.1.9 Provide privacy and security notices consistent with applicable CUI rules.

Does the logon screen display notices upon initial logon?

Yes No Partially Does Not Apply Alternative Approach

Does the system display the system use information before granting access?

Yes No Partially Does Not Apply Alternative Approach

Does the system ensure that any references to monitoring, recording, or auditing are consistent with privacy accommodations?

Yes No Partially Does Not Apply Alternative Approach

Does the system include a description of the authorized uses of the system?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

System use notifications can be implemented using messages or warning banners displayed before individuals log in to information systems. System use notifications are used only for access via logon interfaces with human users and are not required when such human interfaces do not exist. Companies may consider system use notification messages/ banners displayed in multiple languages based on specific company needs and the demographics of information system users.

This requirement references the National Archives and Records Administration's (NARA) Federal Rule 32 CFR 2002 implementing its CUI program. It applies if a specific type of CUI (i.e., information that requires safeguarding or dissemination controls pursuant to law, regulation or Government-wide policy) requires such notices (e.g., before accessing or entering the data. This is not a common situation.

Where to Look:

- information system design documentation
- information system configuration settings and associated documentation
- information system notification messages
- other relevant documents or records

Who to Talk to:

- system/network administrators
- system developers
- employees with information security responsibilities

Perform Test On:

- automated mechanisms implementing access control policy for previous logon notification

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.1.10 Use session lock with pattern-hiding displays to prevent access/viewing of data after period of inactivity.

Is the system configured to lock sessions after a predetermined period of inactivity?

Yes No Partially Does Not Apply Alternative Approach

Is a pattern hiding display used when sessions are locked?

Yes No Partially Does Not Apply Alternative Approach

Can users lock sessions for temporary absence?

Yes No Partially Does Not Apply Alternative Approach

Does the system session lock mechanism place a publicly viewable pattern onto the screen? Hiding what was previously visible on the screen?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

Pattern-hiding display images can include static or dynamic images, for example patterns used with screen savers, photographic images, clock, battery life indicator, or a blank screen with the additional caveat that none of the images convey sensitive information.

Where to Look:

- access control policy
- procedures addressing session lock
- display screen with session lock activated
- procedures addressing identification and authentication
- information system design documentation
- information system configuration settings and associated documentation
- security plan
- other relevant documents or records

Who to Talk to:

- system/network administrators
- employees with information security responsibilities
- system developers

Perform Test On:

- automated mechanisms implementing access control policy for session lock
- information system session lock mechanisms

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.1.11 Terminate (automatically) a user session after a defined condition.

Is the system configured to end a user session after a predetermined period based on duration and/or inactivity of session?

Yes No Partially Does Not Apply Alternative Approach

Are user sessions terminated automatically based upon company defined conditions? For example, 10 minute timeouts?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

This requirement addresses the termination of user-initiated logical sessions in contrast to other requirements that address the termination of network connections that are associated with communications sessions (i.e., network disconnect). A logical session (for local, network, and remote access) is initiated whenever a user (or process acting on behalf of a user) accesses a company information system. Such user sessions can be terminated (and thus terminate user access) without terminating network sessions. Session termination terminates all processes associated with a user's logical session except those processes that are specifically created by the user (i.e., session owner) to continue after the session is terminated. Conditions or trigger events requiring automatic session termination can include, for example, organization-defined periods of user inactivity, targeted responses to certain types of incidents, time-of-day restrictions on information system use.

Where to Look:

- access control policy
- procedures addressing session termination
- information system design documentation
- information system configuration settings and associated documentation
- list of conditions or trigger events requiring session disconnect
- information system audit records
- other relevant documents or records

Who to Talk to:

- system/network administrators
- employees with information security responsibilities
- system developers

Perform Test On:

- automated mechanisms implementing user session termination

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.1.12 Monitor and control remote access sessions.

Does the company allow remote access to the control network?

Yes No Partially Does Not Apply Alternative Approach

Do you run network and system monitoring applications to monitor remote system access and log accordingly?

Yes No Partially Does Not Apply Alternative Approach

Do you control remote access by running only necessary applications?

Yes No Partially Does Not Apply Alternative Approach

Do you use firewalling?

Yes No Partially Does Not Apply Alternative Approach

Do you use end-to-end encryption with appropriate access?

Yes No Partially Does Not Apply Alternative Approach

Are all the methods of remote access to the system authorized, monitored, and managed?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

Remote access is access to a company's IT system by a user communicating through an external network such as the internet.

Remote access client devices generally have weaker protection than standard client devices. These may include:

- Many devices are not managed by the company and do not use enterprise firewalls or antivirus protection.
- A lack of physical security controls when using remote access.
- Remote access client devices may be used in hostile environments but not properly configured for them.
- Remote access communications are carried over untrusted networks.

It is useful to note that one can "monitor and control remote access" by not providing the capability and employing procedural methods to ensure it has not been enabled.

Where to Look:

- access control policy
- procedures addressing remote access to the information system
- information system design documentation
- information system configuration settings and associated documentation
- information system audit records
- information system monitoring records
- other relevant documents or record

Who to Talk to:

- system/network administrators
- employees with information security responsibilities
- system developers

Perform Test On:

- automated mechanisms monitoring and controlling remote access methods

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.1.13 Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.

Do applications used to remotely access the system use approved encryption methods?

Yes No Partially Does Not Apply Alternative Approach

Is cryptography used to protect the confidentiality and integrity of remote access sessions?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

The NIST SP 800-171 requirements for cryptography used to protect the confidentiality of CUI must use Federal Information Processing Standard (FIPS) validated cryptography, which means the cryptographic module has been tested and validated to meet FIPS 140 requirements. Simply using an approved algorithm (e.g., FIPS 197 for AES) is not sufficient – the module (software and/or hardware) used to implement the algorithm must be separately validated under FIPS 140. When an application or device allows a choice (by selecting FIPS-mode or not), then the FIPS-mode has been validated under FIPS 140-2, but the other options (non-FIPS) allow certain operations that would not meet the FIPS requirements. More information is available at http://csrc.nist.gov/groups/STM/cmvp/

When NIST SP 800-171 requires cryptography, it is to protect the confidentiality of CUI. Accordingly, FIPS-validated cryptography is required to protect CUI, typically when transmitted or stored outside the protected environment of the company's information system (including wireless/remote access) if not separately protected (e.g., by a protected distribution system). FIPS-validated cryptography is required whenever the encryption is required to protect covered defense information in accordance with NIST SP 800-171 or by another DFARS contract provision. Encryption used for other purposes, such as within applications or devices within the protected environment of the covered contractor information system, would not need to be FIPS-validated. Note that any separate contract requirement (not currently in NIST SP 800-171) to encrypt data at rest (e.g., Personally Identifiable Information - PII) within the information system would require use of FIPS-validated cryptography.

Where to Look:

- access control policy
- procedures addressing remote access to the information system
- information system design documentation
- information system configuration settings and associated documentation
- cryptographic mechanisms and associated configuration documentation
- information system audit records
- other relevant documents or records

Who to Talk to:

- system/network administrators
- employees with information security responsibilities
- system developers

Perform Test On:

- cryptographic mechanisms protecting confidentiality and integrity of remote access sessions

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.1.14 Route remote access via managed access control points.

Do you allow remote access?

Yes No Partially Does Not Apply Alternative Approach

Is remote access only allowed by authorized methods?

Yes No Partially Does Not Apply Alternative Approach

Is remote access only maintained by your IT department?

Yes No Partially Does Not Apply Alternative Approach

Does the system route all remote access through a limited number of managed access control points?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

Companies should identify and fully define the number of managed network access control points used for remote accesses are routed. All remote access to the system should be routed through these company's managed network access control points.

Where to Look:

- access control policy
- procedures addressing remote access to the information system
- information system design documentation
- list of all managed network access control points
- information system configuration settings and associated documentation
- information system audit records
- other relevant documents or records

Who to Talk to:

- system/network administrators
- employees with information security responsibilities

Perform Test On:

- automated mechanisms routing all remote accesses through managed network access control point

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.1.15 Authorize remote execution of privileged commands and remote access to security-relevant information.

Is remote access for privileged actions (such as software installation) only permitted for necessary operational functions?

Yes No Partially Does Not Apply Alternative Approach

Is remote access for privileged commands and security- relevant information authorized only for compelling operational needs and is the rationale for such access documented?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

This security requirement is intended to limited the use of remote access to perform privileged actions on the system. Privileged commands are human initiated and involve the control, monitoring or administration of the system and security functions.

Where to Look:

- access control policy
- procedures addressing remote access to the information
- information system configuration settings and associated documentation
- security plan
- information system audit records
- other relevant documents or records

Who to Talk to:

- system/network administrators
- employees with information security responsibilities

Perform Test On:

- automated mechanisms implementing remote access management

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.1.16 Authorize wireless access prior to allowing such connections.

Does the company have wireless devices?

Yes No Partially Does Not Apply Alternative Approach

Is the use of wireless technologies approved by company management?

Yes No Partially Does Not Apply Alternative Approach

Is there guidance on the use of wireless technologies?

Yes No Partially Does Not Apply Alternative Approach

Is access to the wireless network restricted to the established guidelines, monitored, and controlled?

Yes No Partially Does Not Apply Alternative Approach

Is wireless access to the system authorized, monitored and managed?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

The use of wireless devices on company systems should be based on management approved guidelines. Access to the wireless network should be monitored and controlled by the company.

Where to Look:

- access control policy
- procedures addressing wireless access implementation and usage (including restrictions)
- configuration management plan
- security plan
- information system design documentation
- information system configuration settings and associated documentation
- wireless access authorizations
- information system audit records
- other relevant documents or records

Who to Talk to:

- employees with responsibilities for managing wireless access connections
- employees with information security responsibilities

Perform Test On:

- wireless access management capability for the information system

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.1.17 Protect wireless access using authentication and encryption.

Is wireless access restricted to authorized users?

Yes No Partially Does Not Apply Alternative Approach

Is wireless access encrypted according to industry best practices?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

The NIST SP 800-171 requirements for cryptography used to protect the confidentiality of CUI must use FIPS-validated cryptography, which means the cryptographic module has been tested and validated to meet FIPS 140 requirements. Simply using an approved algorithm (e.g., FIPS 197 for AES) is not sufficient – the module (software and/ or hardware) used to implement the algorithm must be separately validated under FIPS 140. When an application or device allows a choice (by selecting FIPS-mode or not), then the FIPS-mode has been validated under FIPS 140-2, but the other options (non-FIPS) allow certain operations that would not meet the FIPS requirements. More information is available at

http://csrc.nist.gov/groups/STM/cmvp/

When NIST SP 800-171 requires cryptography, it is to protect the confidentiality of CUI. Accordingly, FIPS-validated cryptography is required to protect CUI, typically when transmitted or stored outside the protected environment of the company's information system (including wireless/remote access) if not separately protected (e.g., by a protected distribution system). FIPS-validated cryptography is required whenever the encryption is required to protect covered defense information in accordance with NIST SP 800-171 or by another DFARS contract provision.

Encryption used for other purposes, such as within applications or devices within the protected environment of the covered contractor information system, would not need to be FIPS-validated. Note that any separate contract requirement (not currently in NIST SP 800-171) to encrypt data at rest (e.g., PII) within the information system would require use of FIPS-validated cryptography.

Where to Look:

- access control policy
- procedures addressing wireless implementation and usage (including restrictions)
- information system design documentation
- information system configuration settings and associated documentation
- information system audit records
- other relevant documents or records

Who to Talk to:

- system/network administrators
- employees with information security responsibilities
- system developers

Perform Test On:

- automated mechanisms implementing wireless access protections to the information system

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.1.18 Control connection of mobile devices.

Has company management established guidelines for the use of mobile devices?

Yes No Partially Does Not Apply Alternative Approach

Does company management restrict the operation of those devices to the guidelines?

Yes No Partially Does Not Apply Alternative Approach

Is usage monitored and controlled?

Yes No Partially Does Not Apply Alternative Approach

Is mobile device connection to the system authorized?

Yes No Partially Does Not Apply Alternative Approach

Are requirements for mobile device connection to the system enforced?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

Mobile devices allow employees to access information resources wherever they are, whenever they need. The small form factor, constant internet access, and powerful mobile applications greatly improve workforce productivity but can pose cybersecurity risks. While many only think of smartphones as mobile devices, companies must consider the security of all mobile network devices including tablets and laptops used as workstations.

NISTIR 8144 "Assessing Threats to Mobile Devices & Infrastructure" describes, identifies, and structures the threats posed to mobile information systems, and can be accessed at https://nccoe.nist.gov/sites/default/files/library/mtc-nistir-8144-draft.pdf

NIST SP 800-124 Rev. 1 "Guidelines for Managing Security of Mobile Devices in the Enterprise" helps organizations centrally manage and secure mobile devices against a variety of threats. It provides recommendations for selecting, implementing, and using centralized management technologies, and it explains the security concerns inherent in mobile device use. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf

Where to Look:

- access control policy
- procedures addressing access control for mobile device usage (including restrictions)
- configuration management plan
- security plan
- information system design documentation
- information system configuration settings and associated documentation
- authorizations for mobile device connections to company information systems
- information system audit records
- other relevant documents or records

Who to Talk to:

- employees using mobile devices to access
- system/network administrators
- employees with information security responsibilities

Perform Test On:

- access control capability authorizing mobile device connections to company information systems

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.1.19 Encrypt CUI on mobile devices.

Are mobile devices encrypted?

Yes No Partially Does Not Apply Alternative Approach

Does the company encrypt CUI on mobile devices?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

The NIST SP 800-171 requirements for cryptography used to protect the confidentiality of CUI must use FIPS-validated cryptography, which means the cryptographic module should have been tested and validated to meet FIPS 140-1 or -2 requirements. Simply using an approved algorithm (e.g., FIPS 197 for AES) is not sufficient - the module (software and/or hardware) used to implement the algorithm must be separately validated under FIPS 140. When an application or device allows a choice (by selecting FIPS-mode or not), then the FIPS-mode has been validated under FIPS 140-2, but the other options (non-FIPS) allow certain operations that would not meet the FIPS requirements. More information is available at

http://csrc.nist.gov/groups/STM/cmvp/

When NIST SP 800-171 requires cryptography, it is to protect the confidentiality of CUI. Accordingly, FIPS-validated cryptography is required to protect CUI, typically when transmitted or stored outside the protected environment of the company's information system (including wireless/remote access) if not separately protected (e.g., by a protected distribution system). FIPS-validated cryptography is required whenever the encryption

is required to protect covered defense information in accordance with NIST SP 800-171 or by another DFARS contract provision. Encryption used for other purposes, such as within applications or devices within the protected environment of the covered contractor information system, would not need to be FIPS-validated. Note that any separate contract requirement (not currently in NIST SP 800-171) to encrypt data at rest (e.g., PII) within the information system would require use of FIPS-validated cryptography.

Where to Look:

- access control policy
- procedures addressing access control for mobile devices
- information system design documentation
- information system configuration settings and associated documentation
- encryption mechanisms and associated configuration documentation
- information system audit records
- other relevant documents or records

Who to Talk to:

- employees with access control responsibilities for mobile devices system/network administrators
- employees with information security responsibilities

Perform Test On:

- encryption mechanisms protecting confidentiality and integrity of information on mobile devices

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.1.20 Verify and control/limit connections to and use of external information systems.

Are only authorized individuals permitted external access?

Yes No Partially Does Not Apply Alternative Approach

Are guidelines and restrictions placed on the use of personally owned or external system access?

Yes No Partially Does Not Apply Alternative Approach

Do those systems meet the security standards set by the company?

Yes No Partially Does Not Apply Alternative Approach

Are the number of access points to the system limited to allow for better monitoring of inbound and outbound network traffic?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

External information systems are information systems or components of information systems that are outside of the authorization boundary established by the company. Companies typically have no direct supervision and authority over the application of security requirements or the assessment of their effectiveness in external information systems. External information systems include, for example: 1) personally owned information systems/devices (e.g., notebook computers, smart phones, tablets, personal digital assistants); 2) privately owned computing and communications devices resident in commercial or public facilities (e.g., hotels, train stations, convention centers, shopping malls, or airports); 3) information systems owned or controlled by nonfederal governmental organizations; and 4) federal information systems that are not owned by, operated by, or under the direct supervision and authority of companies.

Where to Look:

- access control policy procedures addressing the use of external information systems
- external information systems terms and conditions
- list of types of applications accessible from external information systems
- maximum security categorization for information processed, stored, or transmitted on external information systems
- information system configuration settings and associated documentation
- information system connection or processing agreements
- account management documents
- other relevant documents or records

Who to Talk to:

- employees with responsibilities for defining terms and conditions for use of external information systems to access company systems
- system/network administrators
- employees with information security responsibilities

Perform Test On:

- automated mechanisms implementing terms and conditions on use of external information systems
- automated mechanisms implementing limits on use of external information systems

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.1.21 Limit use of organization portable storage devices on external information systems.

Are guidelines and restrictions placed on the use of portable storage devices, e.g., thumb drives?

Yes No Partially Does Not Apply Alternative Approach

Are restrictions imposed on authorized individuals regarding the use of company-controlled removable media on external systems?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

A 'portable storage device' is an information system component that can be inserted into and removed from an information system, and that is used to store data or information (e.g., text, video, audio, and/or image data). Such components are typically implemented on magnetic, optical, or solid-state devices (e.g., floppy disks, compact/digital video disks, flash/thumb drives, external hard disk drives, and flash memory cards/drives that contain non-volatile memory).

Limits on the use of company-controlled portable storage devices in external information systems include, for example, complete prohibition of the use of such devices or restrictions on how the devices may be used and under what conditions the devices may be used.

This requirement is generally implemented by policy, though some devices can be configured to work only when connected to a system to which they can authenticate (this is, however, not a requirement).

Where to Look:

- access control policy
- procedures addressing the use of external information systems
- security plan
- information system configuration settings and associated documentation
- information system connection or processing agreements
- account management documents
- other relevant documents or records

Who to Talk to:

- employees with responsibilities for restricting or prohibiting use of company controlled storage devices on external information systems
- system/network administrators
- employees with information security responsibilities

Perform Test On:

- automated mechanisms restricting use of portable storage devices

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.1.22 Control CUI posted or processed on publicly accessible information systems.

Do only authorized employees post information on publicly accessible information systems?

Yes No Partially Does Not Apply Alternative Approach

Are authorized employees trained to ensure that CUI and non-public information is not posted?

Yes No Partially Does Not Apply Alternative Approach

Is public information reviewed annually to ensure that CUI and non-public information is not posted?

Yes No Partially Does Not Apply Alternative Approach

Is the proposed content of publicly accessible information reviewed prior to posting?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

Improper use of the company's proprietary information can damage the company. Improper use of CUI could cause damage to the government and/or its employees.

This requirement addresses systems that are controlled by the company and accessible to the public, typically without identification or authentication. The posting of information on non-organization information systems is covered by company policy.

DOD uses a variety of markings to identify CUI, identified in DOD Manual 5200.01 Vol 4, which will be updated as the NARA CUI rule (32 CFR 2002) is implemented. The most common form of DOD CUI held by contractors is Controlled Technical Information, which is marked with Distribution Statements B-F. Other DOD information may be marked as 'For Official Use Only' – which may or may not be CUI, and the contracting officer should be consulted if this marking is encountered to determine if it is DOD CUI.

Where to Look:

- access control policy
- procedures addressing publicly accessible content
- list of users authorized to post publicly accessible content on company information systems
- training materials and/or records
- records of publicly accessible information reviews
- records of response to nonpublic information on public websites
- system audit logs
- security awareness training records
- other relevant documents or records

Who to Talk to:

- employees with responsibilities for managing publicly accessible information posted on company information systems
- employees with information security responsibilities

Perform Test On:

- automated mechanisms implementing management of publicly accessible content

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

Awareness and Training: SP 800-171 Security Family 3.2

Users of a system can be viewed as the weakest link in securing systems. Often users are not aware of how their actions may impact the security of a system. Making system users aware of their security responsibilities and teaching them correct practices helps change their behavior. It also supports individual accountability, which is one of the most important ways to improve information security. Without knowing the necessary security measures or how to use them, users cannot be truly accountable for their actions.

The purpose of information security awareness, training, and education is to enhance security by:

- raising awareness of the need to protect system resources,
- developing skills and knowledge so system users can perform their jobs more securely, and
- building in-depth knowledge as needed to design, implement, or operate security programs for organizations and systems.

The company is responsible for making sure that managers and users are aware of the security risks associated with their activities and that employees are trained to carry out their information security-related duties and responsibilities. Examples of awareness and training security requirements include: security awareness training, role based security training, and security training records.

The following security requirements fall under the Awareness and Training family.

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

3.2.1 Ensure that managers, systems administrators, and users of organization information systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of organization information systems.

Do all users, managers, and system administrators receive initial and annual training commensurate with their roles and responsibilities?

Yes No Partially Does Not Apply Alternative Approach

Does the training provide a basic understanding of the need for information security, applicable policies, standards, and procedures related to the security of the information system, as well as user actions to maintain security and respond to suspected security incidents?

Yes No Partially Does Not Apply Alternative Approach

Does the training also address awareness of the need for operations security?

Yes No Partially Does Not Apply Alternative Approach

Is basic security awareness training provided to all system users before authorizing access to the system when required by system changes and at least annually thereafter?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

Companies determine the appropriate content of security awareness training and security awareness techniques based on the specific company requirements and the information systems to which employees have authorized access. The content includes a basic understanding of the need for information security and user actions to maintain security and to respond to suspected security incidents. The content also addresses awareness of the need for operations security. Security awareness techniques can include, for example, displaying posters, offering supplies inscribed with security reminders, generating email advisories/notices from senior company officials, displaying logon screen messages, and conducting information security awareness events.

Where to Look:

- security awareness and training policy
- procedures addressing security awareness training implementation
- appropriate codes of federal regulations
- security awareness training curriculum
- security awareness training materials
- security plan
- training records
- other relevant documents or records

Who to Talk to:

- employees with responsibilities for security awareness training
- employees with information security responsibilities
- employees comprising the general information system user community
- employees with responsibilities for role-based security training

Perform Test On:

- automated mechanisms managing security awareness training
- automated mechanisms managing role-based security training

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.2.2 Ensure that organization personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

Do employees with security-related duties and responsibilities receive initial and annual training on their operational, managerial, and technical roles and responsibilities?

Yes No Partially Does Not Apply Alternative Approach

Does the training cover physical, personnel, and technical safeguards and countermeasures?

Yes No Partially Does Not Apply Alternative Approach

Does the training address required security requirements related to environmental and physical security risks?

Yes No Partially Does Not Apply Alternative Approach

Does the training include indications of potentially suspicious email or web communications?

Yes No Partially Does Not Apply Alternative Approach

Is security-related technical training provided before authorizing access to the system or performing assigned duties, when required by system changes and on a periodic basis?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

Companies determine the appropriate content of security training based on the assigned roles and responsibilities of individuals, and the specific security requirements of companies

and the information systems to which personnel have authorized access. In addition, companies provide enterprise architects, information system developers, software developers, acquisition/ procurement officials, information system managers, system/network administrators, personnel conducting configuration management and auditing activities, personnel performing independent verification and validation activities, security requirement assessors, and other personnel having access to system-level software, adequate security- related technical training specifically tailored for their assigned duties.

Comprehensive role-based training addresses management, operational, and technical roles and responsibilities covering physical, personnel, and technical safeguards and countermeasures. Such training can include for example, policies, procedures, tools, and artifacts for the company security roles defined. Organizations also provide the training necessary for individuals to carry out their responsibilities related to operations and supply chain security within the context of company information security programs. Role-based security training also applies to contractors providing services to federal agencies.

Where to Look:

- security awareness and training policy
- procedures addressing security awareness training implementation
- appropriate codes of federal regulations
- security awareness training curriculum
- security awareness training materials
- security plan training records
- other relevant documents or records

Who to Talk to:

- employees with responsibilities for security awareness training
- employees with information security responsibilities
- employees with responsibilities for role-based security training
- employees with assigned information system security roles and responsibilities
- employees comprising the general information system user community

Perform Test On:

- automated mechanisms managing security awareness training
- automated mechanisms managing role-based security training

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.2.3 Provide security awareness training on recognizing and reporting potential indicators of insider threat.

Do users, managers, and system administrators receive annual training on potential indicators and possible precursors of insider threat, e.g., long-term job dissatisfaction, attempts to gain unauthorized access to information, unexplained access to financial resources, bullying or sexual harassment of fellow employees, workplace violence, and other serious violations of company policies?

Yes No Partially Does Not Apply Alternative Approach

Does security training include how to communicate employee and management concerns regarding potential indicators of insider threat?

Yes No Partially Does Not Apply Alternative Approach

Are practical exercises included in security awareness training that simulate actual cyber-attacks?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

Potential indicators and possible precursors of insider threat can include behaviors such as long-term job dissatisfaction, attempts to gain access to information not required for job performance, unexplained access to financial resources, bullying or sexual harassment of fellow employees, workplace violence, and other serious violations of company policies, procedures, directives, rules, or practice. Security awareness training includes how to communicate employee and management concerns regarding potential indicators of insider threat through appropriate company channels in accordance with established company policies and procedures.

Where to Look:

- security awareness and training policy
- procedures addressing security awareness training implementations
- security awareness training curriculum
- security awareness training materials
- security plan
- other relevant documents or records

Who to Talk to:

- employees who participate in security awareness training
- employees with responsibilities for basic security awareness training
- employees with information security responsibilities

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

Audit and Accountability: SP 800-171 Security Family 3.3

An audit is an independent review and examination of records and activities to assess the adequacy of system requirements and ensure compliance with established policies and operational procedures.

An audit trail is a record of individuals who have accessed a system as well as what operations the user has performed during a given period. Audit trails maintain a record of system activity both by system and application processes and by user activity of systems and applications. In conjunction with appropriate tools and procedures, audit trails can assist in detecting security violations, performance issues, and flaws in applications. Audit trails may be used as a support for regular system operations, a kind of insurance policy, or both. As insurance, audit trails are maintained but not used unless needed (e.g., after a system outage). As a support for operations, audit trails are used to help system administrators ensure that the system or resources have not been harmed by hackers, insiders, or technical problems. Examples of audit and accountability requirements include: audit events, time stamps, nonrepudiation, protection of audit information, audit record retention, and session audit.

Companies should create, protect, and retain system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate system activity and ensure that the actions of users can be uniquely traced to those users so they can be held accountable.

The following security requirements fall under the Audit and Accountability family.

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.3.1 Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity.

Does the system provide alert functions?

Yes No Partially Does Not Apply Alternative Approach

Does the company perform audit analysis and review?

Yes No Partially Does Not Apply Alternative Approach

Does the company create, protect, and retain information system audit records for between 30 days and 1 year (depending on data source and applicable regulations) to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity?

Yes No Partially Does Not Apply Alternative Approach

Are mechanisms used to integrate audit review, analysis, and reporting to processes for investigation and response to suspicious activity?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

It is important for companies to create audit records, protect the integrity of audit records and retain audit records. Good audit records will allow the company to monitor system activities, perform analysis on system activities, provide evidence for use during an investigation and reporting.

Where to Look:

- audit and accountability policy
- procedures addressing content of audit records
- information system design documentation
- procedures addressing audit record generation
- security plan
- list of auditable events
- information system configuration settings and associated documentation
- list of organization-defined auditable events
- information system audit records
- procedures addressing audit review, analysis, and reporting
- reports of audit findings
- records of actions taken in response to reviews/analyses of audit records
- information system incident reports
- other relevant documents or records

Who to Talk to:

- employees with audit and accountability responsibilities
- employees with audit review, analysis, and reporting responsibilities
- employees with information security responsibilities
- system/network administrators
- system developers

Perform Test On:

- automated mechanisms implementing information system auditing of auditable events
- information system audit capability

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.3.2 Ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.

Does the company correlate network activity to individual user information?

Yes No Partially Does Not Apply Alternative Approach

Can the company uniquely trace and hold accountable users responsible for unauthorized actions?

Yes No Partially Does Not Apply Alternative Approach

Does the system protect against an individual denying having performed an action (non-repudiation)?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

Types of individual actions covered by non-repudiation include, for example, creating information, sending and receiving messages, approving information (e.g., indicating concurrence or signing a contract). Non-repudiation protects individuals against later claims by:

- authors of not having authored documents,
- senders of not having transmitted messages,
- receivers of not having received messages, or
- signatories of not having signed documents.

Non-repudiation services can be used to determine if information originated from an individual, or if an individual took specific actions (e.g., sending an email, signing a contract, approving a procurement request) or received specific information. Companies obtain non-repudiation services by employing various techniques or mechanisms (e.g., digital signatures, digital message receipts).

Where to Look:

- audit and accountability policy
- procedures addressing content of audit records
- information system design documentation
- procedures addressing audit record generation
- security plan
- list of auditable events
- information system configuration settings and associated documentation
- list of organization-defined auditable events
- information system audit records
- procedures addressing audit review, analysis, and reporting
- reports of audit findings
- records of actions taken in response to reviews/analyses of audit records
- information system incident reports
- other relevant documents or records

Who to Talk to:

- employees with audit and accountability responsibilities
- employees with audit review, analysis, and reporting responsibilities
- employees with information security responsibilities
- system/network administrators
- system developers

Perform Test On:

- automated mechanisms implementing information system auditing of auditable events
- information system audit capability

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.3.3 Review and update audited events.

Does the company review and update audited events annually or in the event of substantial system changes or as needed?

Yes No Partially Does Not Apply Alternative Approach

Do reviews ensure that the information system can audit events, coordinate with other company entities requiring audit-related information, and provide a rationale for why auditable events are deemed adequate to support security investigations?

Yes No Partially Does Not Apply Alternative Approach

Is the list of defined auditable events reviewed by company management and updated on a regular basis?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

Over time, the events that companies believe should be audited may change. Reviewing and updating the set of audited events periodically is necessary to ensure that the current set is still necessary and sufficient.

Where to Look:

- audit and accountability policy
- procedures addressing auditable events
- security plan
- list of organization-defined auditable events
- auditable events review and update records
- information system audit records
- information system incident reports
- other relevant documents or records

Who to Talk to:

- employees with audit and accountability responsibilities
- employees with information security responsibilities

Perform Test On:

- automated mechanisms supporting review and update of auditable events

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.3.4 Alert in the event of an audit process failure.

Will the system alert employees with security responsibilities in the event of an audit processing failure?

Yes No Partially Does Not Apply Alternative Approach

Does the system maintain audit records on host servers until log delivery to central repositories can be re-established?

Yes No Partially Does Not Apply Alternative Approach

Is there real-time alert when any defined event occurs?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

An accurate and current audit trail is essential for maintaining a record of system activity. If the system fails, employees with security responsibilities must be notified and must take prompt action to correct the problem. Minimally, the system must log this event and the employees with security responsibilities (e.g., system administrator) will receive this notification during the daily system log review. If feasible, active alerting (such as e-mail or paging) should be employed consistent with the company's established operations management systems and procedures.

Where to Look:

- audit and accountability policy
- procedures addressing response to audit processing failures
- information system design documentation
- security plan
- information system configuration settings and associated documentation
- list of personnel to be notified in case of an audit processing failure
- information system audit records
- other relevant documents or records

Who to Talk to:

- employees with audit and accountability responsibilities
- employees with information security responsibilities
- system/network administrator's system developers

Perform Test On:

- automated mechanisms implementing information system response to audit processing failures

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.3.5 Correlate audit review, analysis, and reporting processes for investigation and response to indications of inappropriate, suspicious, or unusual activity.

Does the company use mechanisms across different repositories to integrate audit review, analysis, correlation, and reporting processes?

Yes No Partially Does Not Apply Alternative Approach

Do the mechanisms support processes for investigation and response to suspicious activities, as well as gain company-wide situational awareness?

Yes No Partially Does Not Apply Alternative Approach

Are mechanisms used to integrate audit review, analysis and reporting to processes for investigation and response to suspicious activity?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

Often small companies do a good job of collecting audit information across different platforms but fail to correlate the review, analysis and reporting processes. Providing connections and relationships in the audit information can greatly help in the investigation of and response to suspicious activity on the system.

Where to Look:

- audit and accountability policy
- procedures addressing audit review, analysis, and reporting
- procedures addressing investigation and response to suspicious activities
- information system design documentation
- information system configuration settings and associated documentation
- information system audit records
- information system audit records across different repositories
- other relevant documents or records

Who to Talk to:

- employees with audit review, analysis, and reporting responsibilities
- employees with information security responsibilities

Perform Test On:

- automated mechanisms integrating audit review, analysis, and reporting processes
- automated mechanisms supporting analysis and correlation of audit records

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.3.6 Provide audit reduction and report generation to support on-demand analysis and reporting.

Does the system provide an audit reduction and report generation capability?

Yes No Partially Does Not Apply Alternative Approach

Does it support on-demand audit review, analysis, and reporting requirements and after-the-fact security investigations?

Yes No Partially Does Not Apply Alternative Approach

Does the information system alter the original content or time-ordering of audit records?

Yes No Partially Does Not Apply Alternative Approach

Is there the capability to process audit records for events of interest based on selectable event criteria, such as user identity, event type, location, times, dates, system resources, IP, or information object accessed?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

Audit reduction is a process that manipulates collected audit information and organizes such information in a summary format that is more meaningful to reviewers. Audit reduction and report generation capabilities do not always come from the same information system or from the same company entities conducting auditing activities. Audit reduction capability can include, for example, modern data mining techniques with advanced data filters to identify anomalous behavior in audit records.

The report generation capability provided by the information system can generate customizable reports. Time ordering of audit records can be a significant issue if the details of the timestamp in the record are insufficient.

Where to Look:

- audit and accountability policy
- procedures addressing audit reduction and report generation
- information system design documentation
- information system configuration settings and associated documentation
- audit reduction, review, analysis, and reporting tools
- information system audit records
- other relevant documents or records

Who to Talk to:

- employees with audit reduction and report generation responsibilities
- employees with information security responsibilities

Perform Test On:

- audit reduction and report generation capability

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.3.7 Provide an information system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.

Does the system use internal system clocks to generate time stamps for audit records?

Yes No Partially Does Not Apply Alternative Approach

Can the records time stamps be mapped to UTC (Coordinated Universal Time), compare system clocks with authoritative NTP (Network Time Protocol) servers, and synchronizes system clocks when the time difference is greater than 1 second?

Yes No Partially Does Not Apply Alternative Approach

Does the system synchronize internal system clocks on a defined frequency?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

This provides uniformity of time stamps for information systems with multiple system clocks and systems connected over a network.

Where to Look:

- audit and accountability policy
- procedures addressing time stamp generation information
- system design documentation
- information system configuration settings and associated documentation
- information system audit records
- other relevant documents or records

Who to Talk to:

- employees with information security responsibilities
- system/network administrators
- system developers

Perform Test On:

- automated mechanisms implementing time stamp generation
- automated mechanisms implementing internal information system clock synchronization

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.3.8 Protect audit information and audit tools from unauthorized access, modification, and deletion.

Does the system protect audit information and audit tools from unauthorized access, modification, and deletion?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

This security requirement seeks to prevent a malicious user from erasing all evidence of their activities in the audit information. Only authorized users should have access to audit information and audit tools.

Where to Look:

- audit and accountability policy
- access control policy and procedures
- procedures addressing protection of audit information
- information system design documentation
- information system configuration settings and associated documentation
- information system audit records
- audit tools
- other relevant documents or records

Who to Talk to:

- employees with audit and accountability responsibilities
- employees with information security responsibilities
- system/network administrators
- system developers

Perform Test On:

- automated mechanisms implementing audit information protection

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.3.9 Limit management of audit functionality to a subset of privileged users.

Is access to management of audit functionality authorized only to a limited subset of privileged users?

Yes No Partially Does Not Apply Alternative Approach

Are audit records of nonlocal accesses to privileged accounts and the execution of privileged functions protected?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

Individuals with privileged access to an information system and who are also the subject of an audit by that system, may affect the reliability of audit information by inhibiting audit activities or modifying audit records. This requires that privileged access be further defined between audit-related privileges and other privileges, limiting the users with audit-related privileges.

Where to Look:

- audit and accountability policy
- access control policy and procedures
- procedures addressing protection of audit information
- information system design documentation
- information system configuration settings and associated documentation,
- system-generated list of privileged users with access to management of audit functionality
- access authorizations
- access control list
- information system audit records
- other relevant documents or records

Who to Talk to:

- employees with audit and accountability responsibilities
- employees with information security responsibilities
- system/network administrators

Perform Test On:

- automated mechanisms managing access to audit functionality

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

Configuration Management: SP 800-171 Security Family 3.4

Configuration management is a collection of activities focused on establishing and maintaining the integrity of information technology products and systems through the control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the System Development Life Cycle (SDLC). Configuration management consists of determining and documenting the appropriate specific settings for a system, conducting security impact analyses, and managing changes through a change control board. It allows the entire system to be reviewed to help ensure that a change made on one system does not have adverse effects on another system.

Common secure configurations (also known as security configuration checklists) provide recognized, standardized, and established benchmarks that specify secure configuration settings for information technology platforms and products. Once implemented, checklists can be used to verify that changes to the system have been reviewed from a security point-of-view. A common audit examines the system's configuration to see if major changes (such as connecting to the internet) have occurred that have not yet been analyzed. The NIST checklist repository, maintained as part of the National Vulnerability Database (NVD), provides multiple checklists which can be used to check compliance with the secure configuration specified in the system security plan. The checklists can be accessed at http://web.nvd.nist.gov/view/ncp/repository.

Examples of configuration management requirements include baseline configuration, configuration change control, security impact analysis, least functionality, and software usage restrictions.

Companies establish and maintain baseline configurations and inventories of company systems, including hardware, software, firmware, and documentation throughout the respective SDLC and establish and enforce security configuration settings for information technology products employed in company systems.

The following security requirements fall under the Configuration Management family.

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.4.1 Establish and maintain baseline configurations and inventories of organization information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.

Are baseline configurations developed, documented, and maintained for each information system type?

Yes No Partially Does Not Apply Alternative Approach

Do baseline configurations include software versions and patch level, configuration parameters, network information including topologies, and communications with connected systems?

Yes No Partially Does Not Apply Alternative Approach

Are baseline configurations updated as needed to accommodate security risks or software changes?

Yes No Partially Does Not Apply Alternative Approach

Are baseline configurations developed and approved in conjunction with the Chief Information Security Officer (CISO) or equivalent and the information system owner?

Yes No Partially Does Not Apply Alternative Approach

Are deviations from baseline configurations documented?

Yes No Partially Does Not Apply Alternative Approach

Is the system managed using a system development life-cycle methodology that includes security considerations?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

A well-defined system development life cycle provides the foundation for the successful development, implementation, and operation of company information systems. To apply the required security requirements within the system development life cycle requires a basic understanding of information security, threats, vulnerabilities, adverse impacts, and risk to critical missions/business functions. Security engineering cannot be properly applied if individuals who design, code, and test information systems and system components (including information technology products) do not understand security. It is important that developers include individuals on the development team who possess security expertise and skills to ensure that needed security capabilities are effectively integrated into the information system. Security awareness and training programs can help ensure that individuals having key security roles and responsibilities have the appropriate experience, skills, and expertise to conduct assigned system development life cycle activities. The effective integration of security requirements into enterprise architecture also helps to ensure that important security considerations are addressed early in the system development life cycle and that those considerations are directly related to the company's business processes. This process also enables the integration of the information security architecture into the enterprise architecture, consistent with company risk management and information security strategies.

Where to Look:

- configuration management policy
- procedures addressing the baseline configuration of the information system
- procedures addressing configuration settings for the information system
- configuration management plan
- security plan
- enterprise architecture documentation
- security configuration checklists
- evidence supporting approved deviations from established configuration settings
- change control records
- information system audit records
- information system design documentation
- information system architecture and configuration documentation
- information system configuration settings and associated documentation
- change control records
- other relevant documents or records

Who to Talk to:

- employees with configuration management responsibilities
- employees with security configuration management responsibilities
- employees with information security responsibilities
- system/network administrators

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

Perform Test On:

- processes for managing baseline configurations
- automated mechanisms supporting configuration control of the baseline configuration
- processes for managing configuration settings
- automated mechanisms that implement, monitor, and/or control information system configuration settings
- automated mechanisms that identify and/ or document deviations from established configuration settings

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.4.2 Establish and enforce security configuration settings for information technology products employed in organization information systems.

Are security settings included as part of baseline configurations?

Yes No Partially Does Not Apply Alternative Approach

Do security settings reflect the most restrictive settings appropriate?

Yes No Partially Does Not Apply Alternative Approach

Are changes or deviations to security settings documented?

Yes No Partially Does Not Apply Alternative Approach

Where to Look:

- configuration management policy
- procedures addressing the baseline configuration of the information system
- procedures addressing configuration settings for the information system
- configuration management plan
- enterprise architecture documentation
- information system design documentation
- information system architecture and configuration documentation
- information system configuration settings and associated documentation
- security configuration checklists
- evidence supporting approved deviations from established configuration settings
- system audit records
- change control records
- other relevant documents or records

Who to Talk to:

- employees with configuration management responsibilities
- employees with information security responsibilities
- system/network administrators

Perform Test On:

- processes for managing baseline configurations
- processes for managing configuration settings
- automated mechanisms supporting configuration control of the baseline configuration
- automated mechanisms that implement, monitor, and/or control information system configuration settings
- automated mechanisms that identify and/ or document deviations from established configuration settings

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.4.3 Track, review, approve/disapprove, and audit changes to information systems.

Are changes to the system authorized by company management and documented?

Yes No Partially Does Not Apply Alternative Approach

Are configuration-managed changes to the system audited by company personnel?

Yes No Partially Does Not Apply Alternative Approach

Are changes tracked and documented in an approved IT service management system (ITSM) or equivalent tracking service?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

Changes to information systems include modifications to hardware, software, or firmware components and configuration settings. Companies ensure that testing does not interfere with information system operations. Individuals/groups conducting tests understand company security policies and procedures, information system security policies and procedures, and the specific health, safety, and environmental risks associated with facilities/processes.

Operational systems may need to be taken off-line, or replicated to the extent feasible, before testing can be conducted. If information systems must be taken off-line for testing, the tests are scheduled to occur during planned system outages whenever possible. If testing cannot be conducted on operational systems, organizations employ compensating controls (e.g., testing on replicated systems).

Changes to information systems should be reviewed and approved by company management prior to implementation.

Where to Look:

- configuration management policy
- procedures addressing information system configuration change control
- configuration management plan
- information system architecture and configuration documentation
- security plan
- change control records
- information system audit records change control audit and review reports
- agenda /minutes from configuration change control oversight meetings
- other relevant documents or records

Who to Talk to:

- employees with configuration change control responsibilities
- employees with information security responsibilities
- system/network administrators
- members of change control board or similar

Perform Test On:

- processes for configuration change control
- automated mechanisms that implement configuration change control

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.4.4 Analyze the security impact of changes prior to implementation.

Are changes that affect system security requirements tested prior to implementation?

Yes No Partially Does Not Apply Alternative Approach

Is testing the effectiveness of the changes performed?

Yes No Partially Does Not Apply Alternative Approach

Are only those changes that continue to meet compliance requirements approved and implemented?

Yes No Partially Does Not Apply Alternative Approach

Are configuration changes tested, validated, and documented before installing them on the operational system?

Yes No Partially Does Not Apply Alternative Approach

Has testing been ensured to not interfere with system operations?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

Employees with information security responsibilities (e.g., Information System Administrators, Information System Security Officers, Information System Security Managers, and Information System Security Engineers) conduct security impact analyses. Individuals conducting security impact analyses possess the necessary skills/ technical expertise to analyze the changes to information systems and the associated security ramifications. Security impact analysis may include, for example, reviewing security plans to understand security control requirements and reviewing system design documentation to understand requirement implementation and how specific changes might affect the requirements. Security impact analyses may also include assessments of risk to better understand the impact of the changes and to determine if additional security requirements are required. Security impact analyses are scaled in accordance with the security categories of the information systems.

Where to Look:

- configuration management policy
- procedures addressing security impact analysis for changes to the information system
- configuration management plan
- security impact analysis documentation
- analysis tools and associated outputs
- change control records
- information system audit records
- other relevant documents or records

Who to Talk to:

- employees with responsibility for conducting security impact analysis
- employees with information security responsibilities
- system/network administrators

Perform Test On:

- processes for security impact analysis

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.4.5 Define, document, approve, and enforce physical and logical access restrictions associated with changes to the information system.

Are only employees who are approved to make physical or logical changes on systems allowed to do so?

Yes No Partially Does Not Apply Alternative Approach

Are authorized personnel approved and documented by the service owner and IT security?

Yes No Partially Does Not Apply Alternative Approach

Does all change documentation include the name of the authorized employee making the change?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

Any changes to the hardware, software, and/or firmware components of information systems can potentially have significant effects on the overall security of the systems. Companies should permit only qualified and authorized individuals to access information systems for purposes of initiating changes, including upgrades and modifications.

Companies should maintain records of access to ensure that configuration change control is implemented and to support after-the-fact actions should organizations discover any unauthorized changes. Access restrictions for change also include software libraries. Access restrictions include, for example, physical and logical access controls, workflow automation, media libraries, abstract layers (e.g., changes implemented into third-party interfaces rather than directly into information systems), and change windows (e.g., changes occur only during specified times, making unauthorized changes easy to discover).

Where to Look:

- configuration management policy
- procedures addressing access restrictions for changes to the information system
- configuration management plan
- information system design documentation
- information system architecture and configuration documentation
- information system configuration settings and associated documentation
- logical access approvals
- physical access approvals
- access credentials
- change control records
- information system audit records
- other relevant documents or records

Who to Talk to:

- employees with logical access control responsibilities
- employees with physical access control responsibilities
- employees with information security responsibilities
- system/network administrators

Perform Test On:

- processes for managing access restrictions to change
- automated mechanisms supporting/ implementing/enforcing access restrictions associated with changes to the information system

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.4.6 Employ the principle of least functionality by configuring the information system to provide only essential capabilities.

Is the information system configured to exclude any function not needed in the operational environment?

Yes No Partially Does Not Apply Alternative Approach

Does it deliver one function per system, where practical?

Yes No Partially Does Not Apply Alternative Approach

Does the system employ processing components that have minimal functionality and data storage (e.g., diskless nodes, thin client technologies)?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

Information systems can provide a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential company operations (e.g., key missions, functions). Additionally, it is sometimes convenient to provide multiple services from single information system components, but doing so increases risk over limiting the services provided by any one component. Where feasible, companies should limit component functionality to a single function per device (e.g., email servers or web servers, but not both). Organizations review functions and services provided by information systems or individual components of information systems, to determine which functions and services are candidates for elimination (e.g., VoIP, Instant Messaging, auto-execute, and file sharing).

The deployment of information system components with reduced/minimal functionality reduces the need to secure every user endpoint, and may reduce the exposure of information, information systems, and services to cyber-attacks. It is good practice to block ports or protocols that are not needed in the operational environment. For example, if you do not need or use VoIP, don't allow it.

Where to Look:

- configuration management policy
- configuration management plan
- procedures addressing least functionality in the information system
- security plan
- information system design documentation
- information system configuration settings and associated documentation
- security configuration checklists
- other relevant documents or records

Who to Talk to:

- employees with security configuration management responsibilities
- employees with information security responsibilities
- system/network administrators

Perform Test On:

- processes prohibiting or restricting functions, ports, protocols, and/or services
- automated mechanisms implementing restrictions or prohibition of functions, ports, protocols, and/or services

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.4.7 Restrict, disable, and prevent the use of nonessential programs, functions, ports, protocols, and services.

Are only those ports and protocols necessary to provide the service of the information system configured for that system?

Yes No Partially Does Not Apply Alternative Approach

Are only applications and services that are needed for the function of the system configured and enabled?

Yes No Partially Does Not Apply Alternative Approach

Are systems services reviewed to determine what is essential for the function of that system?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

Information systems can provide a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential company operations (e.g., key missions, functions). Additionally, it is sometimes convenient to provide multiple services from single information system components, but doing so increases risk over limiting the services provided by any one component. Where feasible, companies should limit component functionality to a single function per device (e.g., email servers or web servers, but not both). Organizations review functions and services provided by information systems or individual components of information systems, to determine which functions and services are candidates for elimination (e.g., VoIP, Instant Messaging, auto-execute, and file sharing).

Companies should consider disabling unused or unnecessary physical and logical ports/ protocols (e.g., Universal Serial Bus, File Transfer Protocol, and Hyper Text Transfer Protocol) on information systems to prevent unauthorized connection of devices, unauthorized transfer of information, or unauthorized tunneling. Companies can utilize network scanning tools, intrusion detection and prevention systems, and end-point protections such as firewalls and host-based intrusion detection systems to identify and prevent the use of prohibited functions, ports, protocols, and services.

Where to Look:

- configuration management policy
- procedures addressing least functionality in the information system
- configuration management plan
- security plan
- information system design documentation
- information system configuration settings and associated documentation
- specifications for preventing software program execution
- security configuration checklists
- documented reviews of functions, ports, protocols, and/or services
- change control records
- information system audit records
- other relevant documents or records

Who to Talk to:

- employees with responsibilities for reviewing functions, ports, protocols, and services on the information system
- employees with information security responsibilities
- system/network administrators

Perform Test On:

- processes for reviewing/disabling non-secure functions, ports, protocols, and/or services
- automated mechanisms implementing review and disabling of non-secure functions, ports, protocols, and/or services
- processes preventing program execution on the information system
- processes for software program usage and restrictions
- automated mechanisms preventing program execution on the information system
- automated mechanisms supporting and/or implementing software program usage and restrictions

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.4.8 Apply deny-by-exception (blacklist) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting policy to allow the execution of authorized software.

Is the information system configured to only allow authorized software to run?

Yes No Partially Does Not Apply Alternative Approach

Is the system configured to disallow running unauthorized software?

Yes No Partially Does Not Apply Alternative Approach

Is there a defined list of software programs authorized to execute on the system?

Yes No Partially Does Not Apply Alternative Approach

Is the authorization policy a deny-all, permit by exception for software allowed to execute on the system?

Yes No Partially Does Not Apply Alternative Approach

Is it reviewed at least annually?

Yes No Partially Does Not Apply Alternative Approach

Are automated mechanisms used to prevent program execution in accordance with defined lists (e.g., white listing)?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

The requirements for allowing or disallowing the running of software may include (but not be limited to) the use of firewalls to restrict port access and user operational controls.

The process used to identify software programs that are authorized to execute on company information systems is commonly referred to as whitelisting.

In addition to whitelisting, organizations consider verifying the integrity of white-listed software programs using, for example, cryptographic checksums, digital signatures, or hash functions. Verification of white-listed software can occur either prior to execution or at system startup.

The process used to identify software programs that are not authorized to execute on company information systems is commonly referred to as blacklisting. Organizations can implement blacklisting instead of whitelisting (the stronger of the two policies) is the preferred approach for restricting software program execution.

Policies can also be used to prevent certain types of software from being run on the company's system (e.g., games). Enforcement of these types of policies should be checked by periodic audit. This may provide a simpler approach to meeting this requirement for some companies.

Where to Look:

- configuration management policy
- procedures addressing least functionality in the information system
- configuration management plan
- information system design documentation
- information system configuration settings and associated documentation
- list of software programs not authorized to execute on the information system
- list of software programs authorized to execute on the information system
- security configuration checklists
- review and update records associated with list of unauthorized software programs
- review and update records associated with list of authorized software programs
- change control records
- information system audit records
- other relevant documents or records

Who to Talk to:

- employees with responsibilities for identifying software not authorized to execute on the information system
- employees with responsibilities for identifying software authorized to execute on the information system
- employees with information security responsibilities
- system/network administrators

Perform Test On:

- process for identifying, reviewing, and updating programs not authorized to execute on the information system

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

- process for identifying, reviewing, and updating programs authorized to execute on the information system
- process for implementing blacklisting automated mechanisms supporting and/or implementing blacklisting
- process for implementing whitelisting automated mechanisms supporting and/or implementing whitelisting

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.4.9 Control and monitor user-installed software.

Are user controls in place to prohibit the installation of unauthorized software?

Yes No Partially Does Not Apply Alternative Approach

Is all software in use on the information systems approved?

Yes No Partially Does Not Apply Alternative Approach

Does the company follow good practices which require that user-installed software execute in confined physical or virtual machine environment with limited privileges?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

Approaches to meeting this requirement to control and monitor software installed by users can include policies and procedures. Policies should fully describe what is allowed and procedures should be in place to check that the policy is not violated.

Companies should identify software that may be of greater concern regarding origin or potential for containing malicious code. This requirement is necessary to protect the overall system processing CUI; it is not about software used to actually process CUI.

Where to Look:

- configuration management policy
- procedures addressing user installed software
- configuration management plan
- security plan
- information system design documentation
- information system configuration settings and associated documentation
- information system audit records
- other relevant documents or records

Who to Talk to:

- employees with responsibilities for governing user-installed software
- employees operating, using, and/or maintaining the information system
- employees with information security responsibilities
- system/network administrators
- system developers

Perform Test On:

- processes governing user-installed software on the information system
- automated mechanisms for alerting personnel/roles when unauthorized installation of software is detected

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

Identification and Authentication: SP 800-171 Security Family 3.5

For most systems, identification and authentication is often the first line of defense. Identification is the means of verifying the identity of a user, process, or device, typically as a prerequisite for granting access to resources in a system. Identification and authentication is a technical measure that prevents unauthorized individuals or processes from entering a system. Identification and authentication is a critical building block of information security since it is the basis for most types of access control and for establishing user accountability. Access control often requires that the system can identify and differentiate between users. For example, access control is often based on least privilege, which refers to granting users only those accesses required to perform their duties. User accountability requires linking activities on a system to specific individuals and, therefore, requires the system to identify users. Systems recognize individuals based on the authentication data the systems receive. Authentication presents several challenges: collecting authentication data, transmitting the data securely, and knowing whether the individual who was originally authenticated is still the individual using the system. For example, a user may walk away from a terminal while still logged on, and another person may start using it. There are four means of authenticating a user's identity that can be used alone or in combination.

User identity can be authenticated based on:

- something you know – e.g., a password or Personal Identification Number (PIN),
- something you possess (a token) – e.g., an ATM card or a smart card,
- something you are (static biometric) – e.g., fingerprint, retina, face, ear, DNA, and/or
- something you do (dynamic biometrics) – e.g., voice pattern, handwriting, typing rhythm.

While it may appear that any of these individual methods could provide strong authentication, there are problems associated with each. If an individual wanted to impersonate someone else on a system, they could guess or learn another user's password, or steal or fabricate tokens. Each method also has drawbacks for legitimate users and system administrators: users forget passwords and may lose tokens, and administrative overhead for keeping track of identification and authorization data and tokens can be substantial. Biometric systems have significant technical, user acceptance, and cost problems as well. Examples of identification and authentication requirements include: device identification and authentication, identifier management, authenticator management, authenticator feedback, and re-authentication. Companies should identify 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 company systems.

The following security requirements fall under the Identification and Authentication family.

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.5.1 Identify information system users, processes acting on behalf of users, or devices.

Does the system make use of company-assigned accounts for unique access by individuals?

Yes No Partially Does Not Apply Alternative Approach

If service accounts are necessary for device or process authentication, are the accounts created by the central identity management team and assigned to a member of the team using the account (separation of duties)?

Yes No Partially Does Not Apply Alternative Approach

Are company and service accounts managed centrally and deleted automatically when an individual leaves the company?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

Identification of users is a prerequisite for granting access to resources within the system. It prevents unauthorized individuals or processes from entering the system. Identification and authentication of users is the basis for many types pf access control and user accountability. If this security requirement is not implemented correctly it will impact the remaining Identification and Authentication security requirements.

Where to Look:

- identification and authentication policy
- procedures addressing user identification and authentication
- procedures addressing authenticator management
- information system design documentation
- information system configuration settings and associated documentation
- information system audit records
- list of information system accounts
- list of information system authenticator types
- change-control records associated with managing information system authenticators
- other relevant documents or records

Who to Talk to:

- employees with information system operations responsibilities
- employees with information security responsibilities
- employees with authenticator management responsibilities
- system/network administrators
- employees with account management responsibilities
- system developers

Perform Test On:

- processes for uniquely identifying and authenticating users
- automated mechanisms supporting and/or implementing identification and authentication capability
- automated mechanisms supporting and/or implementing authenticator management capability

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.5.2 Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to company information systems.

Are the accounts in use assigned and managed by the company's central identity management system?

Yes No Partially Does Not Apply Alternative Approach

Are accounts provisioned as part of the established account creation process?

Yes No Partially Does Not Apply Alternative Approach

Are accounts uniquely assigned to new employees, contractors, or subcontractors upon hire?

Yes No Partially Does Not Apply Alternative Approach

Are initial passwords randomly generated strings provided via a password reset mechanism to each employee?

Yes No Partially Does Not Apply Alternative Approach

Is the password reset upon first use?

Yes No Partially Does Not Apply Alternative Approach

Do all passwords follow best practice of at least 12 characters, and require a mix of upper and lower case letters, numbers, and special characters?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

While passwords are commonly used for authentication. There are other more effective methods that can be employed. User identity can be authenticated based on:

- Something the user knows, this may include a password or Personal Identification Number (PIN),
- something the user possesses, a type of token such as an ATM card or a smart card,
- something the user is based on a static biometric such as a fingerprint, retina, face, ear, DNA,
- something the user does based on a dynamic biometric such as a voice pattern, handwriting, or typing rhythm.

Where to Look:

- identification and authentication policy
- procedures addressing user identification and authentication
- procedures addressing authenticator management
- list of information system authenticator types
- change control records associated with managing information system authenticators
- information system design documentation
- information system configuration settings and associated documentation
- information system audit records
- list of information system accounts
- other relevant documents or records

Who to Talk to:

- employees with information system operations responsibilities
- employees with authenticator management responsibilities
- employees with information security responsibilities
- system/network administrators
- employees with account management responsibilities
- system developers

Perform Test On:

- processes for uniquely identifying and authenticating users
- automated mechanisms supporting and/or implementing identification and authentication capability
- automated mechanisms supporting and/or implementing authenticator management capability

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.5.3 Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.

Does the system uniquely identify and authenticate users?

Yes No Partially Does Not Apply Alternative Approach

Is multifactor authentication used for local access to privileged accounts?

Yes No Partially Does Not Apply Alternative Approach

Is multifactor authentication used for network access to privileged accounts?

Yes No Partially Does Not Apply Alternative Approach

Is multifactor authentication used for network access to non-privileged accounts?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

NIST SP 800-171 defines a “privileged user” as “a user that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.”

For example, if users’ computer accounts are “administrator accounts” or have "limited administrative rights” only on their computers, are they considered a “privileged account” requiring multifactor authentication at the “local access level”?

Since, in this case, the "ordinary users" are authorized to perform the function, they are not considered privileged users.

Multifactor authentication (MFA) to an information system uses two or more methods of authentication involving something you know (e.g., password); something you have (e.g., a one-time password generating device like a fob, smart-card, or a mobile app on a smart-phone); and something you are (e.g., biometric like a fingerprint or iris). The traditional authentication method uses a single factor, typically a password, while multifactor authentication requires that a second factor also be used such as a PIN sent via a text message (using something you have – the cell phone) or something you are (fingerprint).

Local Access means access to an organizational system by a user (or process acting on behalf of a user) communicating through a direct connection without the use of a network.

Network Access means access to a system by a user (or a process acting on behalf of a user) communicating through a network (e.g., local area network, wide area network, internet).

1. For a NON-PRIVILEGED user, using a standalone computer (e.g., a laptop computer), with no network access, the access can be via single factor authentication (SFA); MFA is not required. However, if used to connect to a LAN, the network access must be MFA. Typically, organizational desktops are used for network access and so the user must use MFA to access their network account.
2. For a PRIVILEGED user, even local access requires MFA.

MFA is not required to access a mobile device (e.g., smart phones) even if they contain covered defense information, as there is a separate requirement in NIST SP 800-171 (3.1.19) to encrypt CUI on mobile devices and mobile computing platforms, and typically mobile devices do not support MFA in order to access the device. However, if the mobile device is used to access a Covered Contractor Information System, then the system must provide the capability for MFA for access by the device, and which would be entered via the device (e.g., use of a one-time password (OTP) device and a password).

An example: Access to the Army project data requires use of institutional multifactor authentication services. Multifactor authentication to an information system uses two or more methods of authentication involving something you know (e.g., password); something you have (e.g., a One-Time Password generating device like a fob, smart-card, or a mobile app on a smart- phone); and something you are (e.g., a biometric like a fingerprint or iris). New employees assigned to the Army project receive their account and instructions for creating a password from HR during the hiring process. New employees receive notification of their account via registered email with an activation link to set their initial password. Passwords may be reset by contacting the service desk and providing proof of identity, or using the online reset service using pre-defined challenge and response questions. Default passwords for information systems are changed before they are introduced to the network. Passwords are stored centrally in company managed authentication systems (and hashed using hashing algorithms). Encrypted transmission of passwords is required.

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

Where to Look:

- identification and authentication policy
- procedures addressing user identification and authentication
- information system design documentation
- information system configuration settings and associated documentation
- information system audit records
- list of information system accounts
- other relevant documents or records

Who to Talk to:

- employees with information system operations responsibilities
- employees with account management responsibilities
- employees with information security responsibilities
- system/network administrators
- system developers

Perform Test On:

- automated mechanisms supporting and/ or implementing multifactor authentication capability

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.5.4 Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.

Are only anti-replay authentication mechanisms used?

Yes No Partially Does Not Apply Alternative Approach

Are defined replay-resistant authentication mechanisms used for network access to privileged accounts?

Yes No Partially Does Not Apply Alternative Approach

Are defined replay-resistant authentication mechanisms used for network access to non-privileged accounts?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

A replay attack may enable an unauthorized user to gain access. Authentication sessions between the authenticator and the application validating the user credentials must not be vulnerable to a replay attack. An authentication process resists replay attacks (if it is impractical to achieve a successful authentication by recording and replaying a previous authentication message.)

The authentication front-end technologies may include, for example, shibboleth, SSH, Microsoft remote desktop protocol, and SSL VPN. Backend authentication mechanisms in use may include, for example, Kerberos and Active Directory.

Per NIST SP 800-53, Security Controls and Assessment Procedures for Federal Information Systems and Organizations, upon which NIST SP 800-171 is based (and references if additional information is required), "authentication processes resist replay attacks if it is impractical to achieve successful authentications by replaying previous authentication messages. Replay-resistant techniques include, for example, protocols that use nonces or challenges such as Transport Layer Security (TLS) and time synchronous or challenge-response one-time authenticators."

A nonce is a randomly generated value used to defeat "playback" attacks in communication protocols. One party randomly generates a nonce and sends it to the other party. The receiver encrypts it using the agreed upon secret key and returns it to the sender. Because the sender randomly generated the nonce, this defeats playback attacks because the replayer cannot know in advance the nonce the sender will generate. The receiver denies connections that do not have the correctly encrypted nonce.

Where to Look:

- identification and authentication policy
- procedures addressing user identification and authentication
- information system design documentation
- information system configuration settings and associated documentation
- information system audit records
- list of privileged information system accounts
- other relevant documents or records

Who to Talk to:

- employees with information system operations responsibilities
- employees with account management responsibilities
- employees with information security responsibilities
- system/network administrators
- system developers

Perform Test On:

- automated mechanisms supporting and/or implementing identification and authentication capability
- automated mechanisms supporting and/or implementing replay resistant authentication mechanisms

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.5.5 Prevent reuse of identifiers for a defined period.

Are the accounts in use assigned and managed by the company's central identity management system?

Yes No Partially Does Not Apply Alternative Approach

Are accounts provisioned as part of the established account creation process?

Yes No Partially Does Not Apply Alternative Approach

Are accounts uniquely assigned to employees, contractors, and subcontractors?

Yes No Partially Does Not Apply Alternative Approach

Are account identifiers reused?

Yes No Partially Does Not Apply Alternative Approach

Are user account names different than email user accounts?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

Prohibiting the use of information systems account identifiers that are the same as some public identifier such as the individual identifier section of an electronic mail address, this makes it more difficult for adversaries to guess user identifiers on company information system.

Where to Look:

- identification and authentication policy
- procedures addressing identifier management
- procedures addressing account management
- security plan
- information system design documentation
- information system configuration settings and associated documentation
- list of information system accounts
- list of identifiers generated from physical access control devices
- other relevant documents or records

Who to Talk to:

- employees with identifier management responsibilities
- employees with information security responsibilities
- system/network administrators
- system developers

Perform Test On:

- automated mechanisms supporting and/or implementing identifier management

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.5.6 Disable identifiers after a defined period of inactivity.

Are user accounts or identifiers monitored for inactivity?

Yes No Partially Does Not Apply Alternative Approach

Are user or device identifiers disabled after a period of inactivity (e.g., 30 days)?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

Common device identifiers include, for example, media access control (MAC), internet protocol (IP) addresses, or device-unique token identifiers. Management of individual identifiers is not applicable to shared information system accounts (e.g., guest and anonymous accounts). Typically, individual identifiers are the user names of the information system accounts assigned to those individuals. In such instances, the account management activities use account names provided. This requirement also addresses individual identifiers not necessarily associated with information system accounts (e.g., identifiers used in physical security control databases accessed by badge reader systems for access to information systems. Preventing reuse of identifiers implies preventing the assignment of previously used individual, group, role, or device identifiers to different individuals, groups, roles, or devices.

Where to Look:

- identification and authentication policy
- procedures addressing identifier management
- procedures addressing account management
- security plan
- information system design documentation
- information system configuration settings and associated documentation
- list of information system accounts
- list of identifiers generated from physical access control devices
- other relevant documents or records

Who to Talk to:

- employees with identifier management responsibilities
- employees with information security responsibilities
- system/network administrators
- system developers

Perform Test On:

- automated mechanisms supporting and/or implementing identifier management

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.5.7 Enforce a minimum password complexity and change of characters when new passwords are created.

Does the company specify a degree of complexity, e.g., are account passwords a minimum of 12 characters and a mix of upper/lower case, numbers and special characters, including minimum requirements for each type?

Yes No Partially Does Not Apply Alternative Approach

Does the company require a change of characters when new passwords are created?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

The complexity of passwords can protect against brute force attacks.

Where to Look:

- identification and authentication policy
- password policy
- procedures addressing authenticator management
- security plan
- information system design documentation
- information system configuration settings and associated documentation
- password configurations and associated documentation
- other relevant documents or records

Who to Talk to:

- employees with authenticator management responsibilities
- employees with information security responsibilities
- system/network administrators
- system developers

Perform Test On:

- automated mechanisms supporting and/or implementing password-based authenticator management capability

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.5.8 Prohibit password reuse for a specified number of generations.

Can passwords be re-used after a certain number of days or a defined number of password changes?

Yes No Partially Does Not Apply Alternative Approach

Can users re-use the same password when changing their password for at least a certain number of changes?

Yes No Partially Does Not Apply Alternative Approach

Is password reuse prohibited for a defined number of generations?

Yes No Partially Does Not Apply Alternative Approach

Are passwords unique to the organization's systems and not re-used on external information systems?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

The reuse of passwords can greatly dimished the effectiveness of authentication security requirements on the system. While many users may find it convenient to reuse the same password on various systems, this practice can increase the risk of a security incident.

Where to Look:

- identification and authentication policy
- password policy procedures addressing authenticator management
- security plan
- information system design documentation
- information system configuration settings and associated documentation
- password configurations and associated documentation
- other relevant documents or records

Who to Talk to:

- employees with authenticator management responsibilities
- employees with information security responsibilities
- system/network administrators
- system developers

Perform Test On:

- automated mechanisms supporting and/or implementing password-based authenticator management capability

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.5.9 Allow temporary password use for system logons with an immediate change to a permanent password.

Do new employees receive an account and instructions for creating a password during the hiring process?

Yes No Partially Does Not Apply Alternative Approach

Do new employees receive notification of their account, and are they required to reset their initial passwords?

Yes No Partially Does Not Apply Alternative Approach

Are temporary password activation links sent to validated employees should they require a password reset or change?

Yes No Partially Does Not Apply Alternative Approach

Are temporary passwords only good to allow for a password reset?

Yes No Partially Does Not Apply Alternative Approach

Does the system enforce immediate password change after logon when a temporary password is issued, e.g., lost or forgotten password?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

This is the lost or forgotten password situation. The administrator issues a new password where the user can logon and the system will require the user to change the temporary password used to logon.

Where to Look:

- identification and authentication policy
- password policy
- procedures addressing authenticator management
- security plan
- information system design documentation
- information system configuration settings and associated documentation
- password configurations and associated documentation
- other relevant documents or records

Who to Talk to:

- employees with authenticator management responsibilities
- employees with information security responsibilities
- system/network administrators
- system developers

Perform Test On:

- automated mechanisms supporting and/or implementing password-based authenticator management capability

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.5.10 Store and transmit only encrypted representation of passwords.

Are passwords prevented from being stored in reversible encryption form in any company systems?

Yes No Partially Does Not Apply Alternative Approach

Are passwords stored as one-way hashes constructed from passwords?

Yes No Partially Does Not Apply Alternative Approach

Does the company follow the best practice of "salting" hashed passwords?

Yes No Partially Does Not Apply Alternative Approach

Are passwords encrypted in storage and in transmission?

Yes No Partially Does Not Apply Alternative Approach

Additional information:

"Password hashing" performs a one-way transformation on a password, turning the password into another string, called the hashed password. "One-way" means that it is practically impossible to go the other way, i.e., to turn the hashed password back into the original password.

In cryptography, a salt is random data that is used as an additional input to a one-way function that "hashes" a password or passphrase. The primary function of salts is to defend against dictionary attacks or against a pre-computed rainbow table attack. A rainbow table is a precomputed table for reversing cryptographic hash functions, usually for cracking password hashes. Tables are usually used in recovering a plaintext password up to a certain length consisting of a limited set of characters. Salts are used to safeguard passwords in storage. Historically a password was stored in plaintext on a system, but over time, additional safeguards developed to protect a user's password against being read from the system. A new salt is randomly generated for each password and never re-used.

Where to Look:

- identification and authentication policy
- password policy
- procedures addressing authenticator management
- security plan
- information system design documentation
- information system configuration settings and associated documentation
- password configurations and associated documentation
- other relevant documents or records

Who to Talk to:

- employees with authenticator management responsibilities
- employees with information security responsibilities
- system/network administrators
- system developers

Perform Test On:

- automated mechanisms supporting and/or implementing password-based authenticator management capability

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.5.11 Obscure feedback of authentication information.

Do the authentication mechanisms obscure feedback of authentication information during the authentication process?

Yes No Partially Does Not Apply Alternative Approach

Do the authentication mechanisms not return any system specific information such as “wrong password” or “wrong username”?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

This requirement seeks to prevent an observer from viewing authentication information, such as a password, while it is being entered. One technique to obscure feedback is to have dots appear in the password window while it is being typed instead of the actual characters being entered.

The most basic feedback control is never informing the user in an error message what part of the of the authentication transaction failed. In the case of shibboleth, for example, the error message is generic regardless of whether the userid was mistyped, the password was wrong, or (in the case of MFA) there was a problem with the MFA credential provided — the failure simply says that the credentials were invalid. Likewise, unsuccessful authentications at the Kerberos KDCs don’t distinguish between the “principal not found” and the “invalid key” case. LDAP-based authentication interfaces only return a “failure to bind” message from both the main LDAPs and the AD.

Where to Look:

- identification and authentication policy
- password policy
- procedures addressing authenticator management
- security plan
- information system design documentation
- information system configuration settings and associated documentation
- password configurations and associated documentation
- other relevant documents or records

Who to Talk to:

- employees with authenticator management responsibilities
- employees with information security responsibilities
- system/network administrators
- system developers

Perform Test On:

- automated mechanisms supporting and/or implementing password-based authenticator management capability

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

Incident Response: SP 800-171 Security Family 3.6

Systems are subject to a wide range of threat events, from corrupted data files to viruses to natural disasters. Vulnerability to some threat events can be lessened by having standard operating procedures that can be followed in the event of an incident. For example, frequently occurring events like mistakenly deleting a file can usually be repaired through restoration from the backup file. More severe threat events, such as outages caused by natural disasters, are normally addressed in a company's contingency plan. Threat events can also result from a virus, other malicious code, or a system intruder (either an insider or an outsider). They can more generally refer to those incidents that could result in severe damage without a technical expert response. An example of a threat event that would require an immediate technical response would be an organization experiencing a denial-of service attack. This kind of attack would require swift action on the part of the incident response team to reduce the affect the attack will have on the organization. The definition of a threat event is somewhat flexible and may vary by company and computing environment. Although the threats that hackers and malicious code pose to systems and networks are well known, the occurrence of such harmful events remains unpredictable. Security incidents on larger networks (e.g., the internet), such as break-ins and service disruptions, have harmed many companies' computing capabilities. When initially confronted with such incidents, most companies respond in an ad hoc manner. However, recurrence of similar incidents can make it cost-beneficial to develop a standard capability for quick discovery of and response to such events. This is especially true since incidents can often "spread" when left unchecked, thus escalating the damage and seriously harming an organization. Incident handling is closely related to contingency planning. An incident handling capability may be viewed as a component of contingency planning because it allows for the ability to react quickly and efficiently to disruptions in normal processing. Broadly speaking, contingency planning addresses events with the potential to interrupt system operations. Incident handling can be considered that portion of contingency planning specifically that responds to malicious technical threats. Examples of incident response requirements include: incident response training, incident response testing, incident handling, incident monitoring, and incident reporting. Companies should establish an operational incident handling capability for company systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities and track, document, and report incidents to company management and/or authorities.

The following security requirements fall under the Incidence Response family.

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.6.1 Establish an operational incident-handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities.

Is there a company incident response policy which specifically outlines requirements for handling of incidents involving CUI?

Yes No Partially Does Not Apply Alternative Approach

Is an incident handling capability implemented for security incidents that include preparation, detection and analysis, containment, eradication, and recovery?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

Organizations recognize that incident response capability is dependent on the capabilities of company information systems and the business processes being supported by those systems. Companies should consider incident response as part of the definition, design, and development of business processes and information systems. Incident-related information can be obtained from a variety of sources including audit monitoring, network monitoring, physical access monitoring, user/administrator reports, and reported supply chain events. Effective incident handling capability includes coordination among many company entities including, for example, business owners, information system owners, authorizing officials, human resources, physical and personnel security offices, legal departments, operations personnel, and purchasing/procurement offices.

Where to Look:

- incident response policy
- procedures addressing incident response training
- contingency planning policy
- procedures addressing incident handling
- procedures addressing incident monitoring
- procedures addressing incident reporting
- incident response records and documentation
- incident response plan
- contingency plan
- incident response training curriculum
- incident response training materials
- security plan
- incident response training records
- incident reporting records and documentation
- other relevant documents or records

Who to Talk to:

- employees with incident response training and operational responsibilities
- employees with incident handling responsibilities
- employees with incident monitoring responsibilities
- employees with contingency planning responsibilities
- employees with incident reporting responsibilities
- personnel who have/should have reported incidents
- personnel to whom incident information is to be reported
- employees with incident response assistance and support responsibilities
- employees with access to incident response support and assistance capability
- employees with information security responsibilities

Perform Test On:

- incident handling capability for the company
- automated mechanisms supporting and/or implementing tracking and documenting of system security incidents
- processes for incident reporting
- automated mechanisms supporting and/or implementing incident reporting
- processes for incident response assistance
- automated mechanisms supporting and/or implementing incident response assistance

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.6.2 Track, document, and report incidents to appropriate officials and/or authorities both internal and external to the organization.

Is there a company incident response policy which specifically outlines requirements for tracking and reporting of incidents involving CUI to appropriate officials?

Yes No Partially Does Not Apply Alternative Approach

Is cybersecurity incident information promptly reported to company management and authorities?

Yes No Partially Does Not Apply Alternative Approach

Are security incidents related to industrial control systems security incidents promptly reported to company management and authorities?

Yes No Partially Does Not Apply Alternative Approach

Are employees required to report suspected security incidents to the company's incident response authority within a defined time-period?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

The intent of this requirement is to address both specific incident reporting requirements within a company and incident reporting requirements that are external to the company. Suspected security incidents include, for example, the receipt of suspicious email communications that can potentially contain malicious code. The types of security incidents reported, the content and timeliness of the reports, and the designated reporting authorities reflect applicable laws, directives, regulations, policies, standards, and guidance.

Where to Look:

- incident response policy
- procedures addressing incident response training
- incident response training curriculum
- incident response training materials
- procedures addressing incident response assistance
- contingency planning policy
- procedures addressing incident handling
- procedures addressing incident monitoring
- incident response records and documentation
- procedures addressing incident reporting
- incident reporting records and documentation
- contingency plan
- security plan
- incident response plan
- incident response training records
- other relevant documents or records

Who to Talk to:

- employees with incident response training and operational responsibilities
- employees with information security responsibilities
- employees with incident handling responsibilities
- employees with contingency planning responsibilities
- employees with incident monitoring responsibilities
- employees with incident reporting responsibilities
- personnel who have/should have reported incidents
- personnel (authorities) to whom incident information is to be reported
- personnel with incident response assistance and support responsibilities
- employees with access to incident response support and assistance capability
- employees with information security responsibilities

Perform Test On:

- incident handling capability for the organization
- incident monitoring capability for the organization
- automated mechanisms supporting and/or implementing tracking and documenting of system security incidents
- processes for incident reporting
- automated mechanisms supporting and/or implementing incident reporting
- processes for incident response assistance

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

- automated mechanisms supporting and/or implementing incident response assistance

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.6.3 *Test the organization incident response capability.*

Is there a company incident response policy?

Yes No Partially Does Not Apply Alternative Approach

Does it outline requirements for regular testing and reviews/improvements to incident response capabilities?

Yes No Partially Does Not Apply Alternative Approach

Does the company test its incident response capabilities?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

Companies test incident response capabilities to determine the effectiveness of the capabilities and to identify potential weaknesses or deficiencies. Incident response testing includes the use of checklists, walk-through or tabletop exercises, simulations (parallel/full interrupt), and comprehensive exercise. Incident response testing can also include a determination of the effects on company operations (e.g., reduction in production capabilities), company assets, and individuals due to incident response.

Where to Look:

- incident response policy
- contingency planning policy
- procedures addressing incident response testing
- procedures addressing contingency plan testing
- incident response testing material
- incident response testing results
- incident response testing plan
- incident response testing documentation
- business continuity plans
- disaster recovery plans
- continuity of operations plans
- crisis communications plan
- critical infrastructure plans
- occupant emergency plan
- incident response plan
- contingency plan
- security plan
- other relevant documents or records

Who to Talk to:

- employees with incident response testing responsibilities
- employees with responsibilities for testing company plans related to incident response testing
- employees with information security responsibilities

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

Maintenance: SP 800-171 Security Family 3.7

To keep systems in good working order and to minimize risks from hardware and software failures, it is important that companies establish procedures for systems maintenance. There are many ways a company can address these maintenance requirements. Controlled maintenance of a system deals with maintenance that is scheduled and performed in accordance with the manufacturer's specifications. Maintenance performed outside of a scheduled cycle, known as corrective maintenance, occurs when a system fails or generates an error condition that must be corrected to return the system to operational conditions. Maintenance can be performed locally or non-locally. Nonlocal maintenance is any maintenance or diagnostics performed by individuals communicating through a network either internally or externally (e.g., the internet). Examples of maintenance requirements include: controlled maintenance, maintenance tools, nonlocal maintenance, maintenance personnel, and timely maintenance. Companies should perform periodic and timely maintenance on company systems and provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.

The following security requirements fall under the Maintenance family.

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.7.1 Perform maintenance on organization information systems.

Are IT system maintenance tools (e.g., tools used for diagnostics, scanner and patching tools) managed?

Yes No Partially Does Not Apply Alternative Approach

Is there a list of approved tools and their access and location is controlled?

Yes No Partially Does Not Apply Alternative Approach

Are all systems, devices, and supporting systems for the company maintained per manufacturer recommendations or company defined schedules?

Yes No Partially Does Not Apply Alternative Approach

Does the company perform maintenance on the information system?

Yes No Partially Does Not Apply Alternative Approach

Does company management approve maintenance activities?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

In general, system maintenance requirements tend to support the security objective of availability. However, improper system maintenance or a failure to perform maintenance can result in the unauthorized disclosure of CUI, thus compromising confidentiality of that information.

This requirement refers to the maintenance of company IT systems.

Where to Look:

- information system maintenance policy
- procedures addressing controlled information system maintenance
- maintenance records
- manufacturer/vendor maintenance specifications
- equipment sanitization records
- media sanitization records
- procedures addressing information system maintenance tools
- maintenance tool inspection records
- information system maintenance tools and associated documentation
- other relevant documents or records

Who to Talk to:

- employees with information system maintenance responsibilities
- employees with information security responsibilities
- employees responsible for media sanitization
- system/network administrators

Perform Test On:

- processes for scheduling, performing, documenting, reviewing, approving, and monitoring maintenance and repairs for the information system
- processes for sanitizing information system components
- automated mechanisms supporting and/or implementing controlled maintenance
- automated mechanisms implementing sanitization of information system components
- processes for approving, controlling, and monitoring maintenance tools
- automated mechanisms supporting and/ or implementing approval, control, and/or monitoring of maintenance tools
- processes for inspecting maintenance tools
- automated mechanisms supporting and/or implementing inspection of maintenance tools
- process for inspecting media for malicious code
- automated mechanisms supporting and/or implementing inspection of media used for maintenance

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.7.2 Provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.

Are controls in place that limit the tools, techniques, mechanisms, and employees used to maintain information systems, devices, and supporting systems?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

This requirement seeks to manage issues that can arise from the misuse of tools, techniques, and mechanisms that are used for IT system maintenance. Diagnostic tools and software can introduce malware into company systems if not managed properly. Employees with IT maintenance responsibilities can behave in a malicious manner if not supervised and managed effectively.

Controls may include lists of authorized tools, authorized employees, and authorized techniques and mechanisms. Any such maintenance must occur within the context of other information systems controls in place.

Where to Look:

- information system maintenance policy
- procedures addressing controlled information system maintenance
- procedures addressing information system maintenance tools
- information system maintenance tools and associated documentation
- maintenance tool inspection records
- maintenance records
- manufacturer/vendor maintenance specifications
- equipment sanitization records
- media sanitization records
- other relevant documents or records

Who to Talk to:

- employees with information system maintenance responsibilities
- employees with information security responsibilities
- employees responsible for media sanitization system/network administrators

Perform Test On:

- processes for scheduling, performing, documenting, reviewing, approving, and monitoring maintenance and repairs for the information system
- processes for sanitizing information system components automated mechanisms supporting and/or implementing controlled maintenance
- automated mechanisms implementing sanitization of information system components
- processes for approving, controlling, and monitoring maintenance tools
- automated mechanisms supporting and/ or implementing approval, control, and/or monitoring of maintenance tools
- processes for inspecting maintenance tools
- automated mechanisms supporting and/or implementing inspection of maintenance tools
- process for inspecting media for malicious code
- automated mechanisms supporting and/or implementing inspection of media used for maintenance

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.7.3 Ensure equipment removed for off-site maintenance is sanitized of any CUI.

Is there a company media sanitization policy?

Yes No Partially Does Not Apply Alternative Approach

Are media that are removed from the premises for maintenance, repair, or disposal sanitized per the company's media sanitization policies?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

This requirement addresses the information security aspects of the information system maintenance program and applies to all types of maintenance to any system component (including applications) conducted by any local or nonlocal entity (e.g., in-contract, warranty, in-house, software maintenance agreement). System maintenance also includes those components not directly associated with information processing and/or data/information retention such as scanners, copiers, and printers. Information necessary for creating effective maintenance records includes: date and time of maintenance, name of individuals or group performing the maintenance, name of escort (if necessary), a description of the maintenance performed, and information system components/equipment removed or replaced (including identification numbers, if applicable). Companies should consider supply chain issues associated with replacement components for information systems.

Where to Look:

- media sanitization policy
- information system maintenance policy
- procedures addressing controlled information system maintenance
- maintenance records
- manufacturer/vendor maintenance specifications
- equipment sanitization records
- media sanitization records
- other relevant documents or records

Who to Talk to:

- employees with information system maintenance responsibilities
- employees with information security responsibilities
- employees responsible for media sanitization
- system/network administrators

Perform Test On:

- processes for scheduling, performing, documenting, reviewing, approving, and monitoring maintenance and repairs for the information system
- processes for sanitizing information system components
- automated mechanisms supporting and/or implementing controlled maintenance
- automated mechanisms implementing sanitization of information system components

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.7.4 Check media containing diagnostics and test programs for malicious code before the media are used in the information system.

Are media that are provided by authorized maintenance personnel (and not normal systems administrators/owners) for troubleshooting, diagnostics, or other maintenance run through an anti-virus/anti-malware/anti-spyware program prior to use in the company's information system?

Yes No Partially Does Not Apply Alternative Approach

Are the results of the scans documented in the maintenance logs?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

Malicious code is often introduced to a system by media used for diagnostic or testing purposes. All media provided by authorized maintenance personnel should be scanned for malware.

Where to Look:

- information system maintenance policy
- procedures addressing information system maintenance tools
- information system maintenance tools and associated documentation
- maintenance records
- other relevant documents or records

Who to Talk to:

- employees with information system maintenance responsibilities
- employees with information security responsibilities

Perform Test On:

- process for inspecting media for malicious code
- automated mechanisms supporting and/or implementing inspection of media used for maintenance

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.7.5 Require multifactor authentication to establish non-local maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.

Does all remote access to a system for maintenance or diagnostics occur via an approved remote solution using multifactor authentication?

Yes No Partially Does Not Apply Alternative Approach

Does the system require multifactor authentication for remote access?

Yes No Partially Does Not Apply Alternative Approach

Are all sessions and remote connections terminated when remote maintenance is completed?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

Non-local maintenance and diagnostic activities are those activities conducted by individuals communicating through a network, either an external network (e.g., the internet) or an internal network. Local maintenance and diagnostic activities are those activities carried out by individuals physically present at the information system or information system component and not communicating across a network connection. Typically, strong authentication requires authenticators that are resistant to replay attacks and employ multifactor authentication. Strong authenticators include, for example, PKI where certificates are stored on a token protected by a password, passphrase, or biometric.

The multifactor authentication for non-local maintenance is intended for recurring non-local maintenance by organizational personnel rather than episodic non-local maintenance by outside vendors where issuance of such credentials for one-time activities is not efficient and may not be advisable. Presuming the individual performing the repair is known and trusted, it is possible to provide for "one-time" multifactor authentication using a password and a separately provided token (e.g., PIN via text message to a cell phone).

Where to Look:

- information system maintenance policy
- procedures addressing nonlocal information system maintenance
- security plan
- system design documentation
- information system configuration settings and associated documentation
- maintenance records
- diagnostic records
- other relevant documents or records

Who to Talk to:

- employees with information system maintenance responsibilities
- employees with information security responsibilities
- system/network administrators

Perform Test On:

- processes for managing nonlocal maintenance
- automated mechanisms implementing, supporting, and/or managing nonlocal maintenance
- automated mechanisms for strong authentication of nonlocal maintenance diagnostic sessions
- automated mechanisms for terminating nonlocal maintenance sessions and network connections

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization.

Are all activities of maintenance personnel (who do not normally have access to a system) monitored?

Yes No Partially Does Not Apply Alternative Approach

Has the company defined approved methods for supervision?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

Escorting maintenance personnel while they work in company facilities can provide a level of supervision over their activities.

Where to Look:

- information system maintenance policy
- procedures addressing maintenance personnel
- service provider contracts service-level agreements
- list of authorized personnel
- maintenance records
- access control records
- other relevant documents or records

Who to Talk to:

- employees with information system maintenance responsibilities
- employees with information security responsibilities

Perform Test On:

- processes for authorizing and managing maintenance personnel
- automated mechanisms supporting and/or implementing authorization of maintenance personnel

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

Media Protection: SP 800-171 Security Family 3.8

Media protection is a requirement that addresses the defense of system media, which can be described as both digital and non-digital. Examples of digital media include: diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Examples of non-digital media include paper or microfilm. Media protections can restrict access and make media available to authorized personnel only, apply security labels to sensitive information, and provide instructions on how to remove information from media so that the information cannot be retrieved or reconstructed. Media protections also include physically controlling system media and ensuring accountability, as well as restricting mobile devices capable of storing and carrying information into or outside of restricted areas. Examples of media protection requirements include: media access, media marking, media storage, media transport, and media sanitization. Companies should protect system media, both paper and digital, limit access to information on system media to authorized users, and sanitize or destroy system media before disposal or release for reuse.

The following security requirements fall under the Media Protection family.

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.8.1 Protect (i.e., physically control and securely store) information system media containing CUI, both paper and digital.

Have responsible parties for data in these systems documented and ensured proper authorization controls for data in media and print?

Yes No Partially Does Not Apply Alternative Approach

Are documented workflow, data access controls, and media policy enforced to ensure proper access controls?

Yes No Partially Does Not Apply Alternative Approach

Is the system media securely stored in protected areas?

Yes No Partially Does Not Apply Alternative Approach

Do only approved individuals have access to media from CUI systems?

Yes No Partially Does Not Apply Alternative Approach

Is an audit log of any media removed from these systems?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

Physically controlling information system media includes, for example, conducting inventories, ensuring procedures are in place to allowindividuals to check out and return media to the media library, and maintaining accountability for all stored media. Secure storage includes, for example, a locked drawer, desk, or cabinet, or a controlled media library. The type of media storage is commensurate with the security category and/or classification of the information residing on the media. Controlled areas are areas for which companies provide sufficient physical and procedural safeguards to meet the requirements established for protecting information and/or information system. For media containing information determined by companies to be in the public domain, to be publicly releasable, or to have limited or no adverse impact on the company or individuals if accessed by other than authorized personnel, fewer safeguards may be needed. In these situations, physical access controls provide adequate protection.

Where to Look:

- information system media protection policy
- procedures addressing media access restrictions
- procedures addressing media storage
- audit records
- information system design documentation
- information system configuration settings and associated documentation
- physical and environmental protection plan
- access control policy and procedures
- physical and environmental protection policy and procedures
- media storage facilities access control records
- security plan
- information system media designated controlled areas
- other relevant documents or records

Who to Talk to:

- employees with information system media protection responsibilities
- employees with information system media storage responsibilities
- employees with information security responsibilities
- system/network administrators

Perform Test On:

- processes for restricting information media
- automated mechanisms supporting and/or implementing media access restrictions
- processes for storing information media
- automated mechanisms supporting and/or implementing secure media storage/media protection
- processes for media sanitization
- automated mechanisms supporting and/or implementing media sanitization

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.8.2 Limit access to CUI on information system media to authorized users.

Are all CUI systems managed under least access rules?

Yes No Partially Does Not Apply Alternative Approach

Does the company limit CUI media access to authorized users?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

Physically controlling information system media includes, for example, conducting inventories, ensuring procedures are in place to allow individuals to check out and return media to the media library, and maintaining accountability for all stored media. Secure storage includes, for example, a locked drawer, desk, or cabinet, or a controlled media library. The type of media storage is commensurate with the security category and/or classification of the information residing on the media. Controlled areas are areas for which companies provide sufficient physical and procedural safeguards to meet the requirements established for protecting information and/or information systems. For media containing information determined by companies to be in the public domain, to be publicly releasable, or to have limited or no adverse impact on the company or individuals if accessed by other than authorized personnel, fewer safeguards may be needed. In these situations, physical access controls provide adequate protection.

Where to Look:

- information system media protection policy
- procedures addressing media access restrictions
- access control policy and procedures
- procedures addressing media storage
- media sanitization and disposal plan
- media sanitization policy
- media sanitization records
- audit records
- information system design documentation
- information system configuration settings and associated documentation
- security plan
- information system media designated controlled areas
- physical and environmental protection policy and procedures
- media storage facilities access control records
- other relevant documents or records

Who to Talk to:

- employees with information system media protection responsibilities
- employees with information system media protection and storage responsibilities
- employees with media sanitization responsibilities
- employees with information security responsibilities
- system/network administrators

Perform Test On:

- processes for restricting information media
- automated mechanisms supporting and/or implementing media access restrictions
- processes for storing information media
- automated mechanisms supporting and/or implementing secure media storage/media protection
- processes for media sanitization
- automated mechanisms supporting and/or implementing media sanitization

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.8.3 Sanitize or destroy information system media containing CUI before disposal or release for reuse.

Is all managed data storage erased, encrypted, or destroyed using mechanisms to ensure that no usable data is retrievable?

Yes No Partially Does Not Apply Alternative Approach

Is system digital and non-digital media sanitized before disposal or release for reuse?

Yes No Partially Does Not Apply Alternative Approach

Are all CUI data on media encrypted or physically locked prior to transport outside of the company's secure locations?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

This requirement applies to all information system media, both digital and nondigital, subject to disposal or reuse, whether or not the media is considered removable. Examples include media found in scanners, copiers, printers, notebook computers, workstations, network components, and mobile devices. The sanitization process removes information from the media such that the information cannot be retrieved or reconstructed. Sanitization techniques, including clearing, purging, cryptographic erase, and destruction, prevent the disclosure of information to unauthorized individuals when such media is reused or released for disposal. Companies should determine the appropriate sanitization methods recognizing that destruction is sometimes necessary when other methods cannot be applied to media requiring sanitization. Companies may use discretion on the employment of approved sanitization techniques and procedures for media containing information deemed to be in the public domain or publicly releasable, or deemed to have no adverse impact on organizations or individuals if released for reuse or disposal.

NIST SP 800-88 "Guidelines for Media Sanitization" provides useful information that will assist companies in implementing a media sanitization program with proper and applicable techniques and controls for sanitization and disposal decisions, available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf.

Where to Look:

- information system media protection policy
- procedures addressing media access restrictions
- procedures addressing media storage
- procedures addressing media sanitization and disposal
- media sanitization policy
- media sanitization records
- audit records
- information system design documentation
- information system configuration settings and associated documentation
- security plan
- information system media designated controlled areas
- access control policy and procedures
- physical and environmental protection policy and procedures
- media storage facilities access control records
- other relevant documents or records

Who to Talk to:

- employees with information system media protection responsibilities
- employees with information security responsibilities
- employees with media sanitization responsibilities
- employees with information system media protection and storage responsibilities
- system/network administrators

Perform Test On:

- processes for restricting information media
- automated mechanisms supporting and/or implementing media access restrictions
- processes for storing information media
- automated mechanisms supporting and/or implementing secure media storage/media protection
- processes for media sanitization
- automated mechanisms supporting and/or implementing media sanitization

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.8.4 Mark media with necessary CUI markings and distribution limitations.

Are all CUI systems identified with an asset control identifier, for example, does each company laptop have an asset id tag with a unique number?

Yes No Partially Does Not Apply Alternative Approach

Are removable system media and system output marked?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

The term security marking refers to the application/use of human-readable security attributes. The term security labeling refers to the application/use of security attributes regarding internal data structures within information systems. Security marking is generally not required for media containing information determined by companies to be in the public domain or to be publicly releasable. However, some companies may require markings for public information indicating that the information is publicly releasable.

This security requirement is meant to be applied by using physical controls to access physical media, but other mechanisms for logical access are acceptable. It applies to information system media, which includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/ removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. It does not include cell or smartphones.

The requirements of the DFARS clause only apply to covered defense information, i.e., information provided or developed by the contractor for DOD which is Controlled Technical Information or other information requiring protection by law, regulation, or government-wide policy. It does not apply to information provided by or developed for non- DOD organizations. Guidance on marking media, along with other materials, should be addressed separately in the contract and is derived from DOD Manual 5200.01, Volume 4, "DOD Information Security Program: Controlled Unclassified Information (CUI).

Where to Look:

- information system media protection policy
- procedures addressing media marking
- physical and environmental protection policy and procedures
- security plan
- list of information system media marking security attributes
- designated controlled areas
- other relevant documents or records

Who to Talk to:

- employees with information system media protection and marking responsibilities
- employees with information security responsibilities

Perform Test On:

- processes for marking information media
- automated mechanisms supporting and/or implementing media marking

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.8.5 Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.

Do only approved individuals have access to media from CUI systems?

Yes No Partially Does Not Apply Alternative Approach

Is an audit log of any media removed from these systems?

Yes No Partially Does Not Apply Alternative Approach

Is accountability for system media maintained during transport outside controlled areas?

Yes No Partially Does Not Apply Alternative Approach

Are all CUI data on media encrypted or physically locked prior to transport outside of the company's secure locations?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

This requirement also applies to mobile devices with information storage capability (e.g., smart phones, tablets, E-readers), that are transported outside of controlled areas. Controlled areas are areas or spaces for which organizations provide sufficient physical and/or procedural safeguards to meet the requirements established for protecting information and/or information systems.

Safeguards to protect media during transport include, for example, locked rooms, containers, and cryptography. Cryptographic mechanisms can provide confidentiality and integrity protections depending upon the mechanisms used. Activities associated with transport include the actual transport as well as those activities such as releasing media for transport and ensuring that media enters the appropriate transport processes.

For the actual transport, authorized transport and courier personnel may include individuals from outside the organization (e.g., U.S. Postal Service or a commercial transport or delivery service). Maintaining accountability of media during transport includes, for example, restricting transport activities to authorized personnel, and tracking and/or obtaining explicit records of transport activities as the media moves through the transportation system to prevent and detect loss, destruction, or tampering. Companies should establish documentation requirements for activities associated with the transport of information system media in accordance with company assessments of risk to include the flexibility to define different record-keeping methods for the different types of media transport as part of an overall system of transport-related records.

Where to Look:

- information system media protection policy
- procedures addressing media storage
- physical and environmental protection policy and procedures
- access control policy and procedures
- security plan
- information system media designated controlled areas
- other relevant documents or records

Who to Talk to:

- employees with information system media protection and storage responsibilities
- employees with information security responsibilities
- system/network administrators

Perform Test On:

- processes for storing information media
- automated mechanisms supporting and/or implementing media storage/media protection

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.8.6 Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.

Are all CUI data on media encrypted or physically locked prior to transport outside of the company?

Yes No Partially Does Not Apply Alternative Approach

Are cryptographic mechanisms used to protect digital media during transport outside of controlled areas?

Yes No Partially Does Not Apply Alternative Approach

Does removable media support physical encryption?

Yes No Partially Does Not Apply Alternative Approach

Is key vaulting utilized to ensure recoverability?

Yes No Partially Does Not Apply Alternative Approach

Are data backups encrypted on media before removal from the company's secured facility?

Yes No Partially Does Not Apply Alternative Approach

Do cryptographic mechanisms comply with FIPS 140-2?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

This requirement also applies to mobile computing and communications devices with information storage capability (e.g., notebooks/ laptop computers, personal digital assistants, cell/smart phones, digital cameras and audio recording devices) that are transported outside of controlled areas. Telephone systems are also considered information systems and may have the capability to store information on internal media (e.g., on voicemail).

Key vaults help safeguard cryptographic keys and secrets systems, applications, and services. By using a key vault, you can encrypt keys and secrets (such as authentication keys, storage account keys, data encryption keys, and passwords) by using keys that are protected by hardware security modules (HSMs). For added assurance, you can import or generate keys in HSMs. Key vaults streamline the key management process and enables you to maintain control of keys that access and encrypt your data.

Where to Look:

- information system media protection policy
- procedures addressing media transport
- information system design documentation
- information system configuration settings and associated documentation
- information system media transport records
- audit records
- other relevant documents or records

Who to Talk to:

- employees with information system media transport responsibilities
- employees with information security responsibilities

Perform Test On:

- cryptographic mechanisms protecting information on digital media during transportation outside controlled areas

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.8.7 Control the use of removable media on information system components.

Is the use of writable, removable media restricted on the system?

Yes No Partially Does Not Apply Alternative Approach

Are removable media allowed?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

Removable media will only be allowed if there are processes in place to control them. Removable media must be able to support physical encryption, and key vaulting must be utilized to ensure recoverability.

The use of non-digital media such as paper files should also be controlled.

Where to Look:

- information system media protection policy
- system use policy
- procedures addressing media usage restrictions
- security plan
- rules of behavior
- information system design documentation
- information system configuration settings and associated documentation
- audit records
- other relevant documents or records

Who to Talk to:

- employees with information system media use responsibilities
- employees with information security responsibilities system/network administrators

Perform Test On:

- processes for media use
- automated mechanisms prohibiting use of media on information systems or system components

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.8.8 Prohibit the use of portable storage devices when such devices have no identifiable owner.

Do all portable storage devices have identifiable owners?

Yes No Partially Does Not Apply Alternative Approach

Have unused removable media that contain support files been removed or disabled?

Yes No Partially Does Not Apply Alternative Approach

Are only approved portable storage devices under asset management used to store CUI data?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

Only approved portable storage devices under asset management are to be used to store CUI data. Portable storage devices are small hard drives designed to hold digital data.

Requiring identifiable owners (e.g., individuals, organizations, or projects) for portable storage devices reduces the risk of using such technologies by allowing organizations to assign responsibility and accountability for addressing known vulnerabilities in the devices (e.g., malicious code insertion).

Where to Look:

- information system media protection policy
- system use policy
- procedures addressing media usage restrictions
- security plan
- rules of behavior
- information system design documentation
- information system configuration settings and associated documentation
- audit records
- other relevant documents or records

Who to Talk to:

- employees with information system media use responsibilities
- employees with information security responsibilities
- system/network administrators

Perform Test On:

- processes for media use
- automated mechanisms prohibiting use of media on information systems or system components

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.8.9 Protect the confidentiality of backup CUI at storage locations.

Are data backups encrypted on media before removal from a secured facility?

Yes No Partially Does Not Apply Alternative Approach

Is the confidentiality and integrity of backup information protected at the storage location?

Yes No Partially Does Not Apply Alternative Approach

Are data backups encrypted on media before removal from the company's secured facility?

Yes No Partially Does Not Apply Alternative Approach

Do cryptographic mechanisms comply with FIPS 140-2?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

System-level information includes, for example, system-state information, operating system and application software, and licenses. User-level information includes any information other than system-level information. Mechanisms employed by companies to protect the integrity of information system backups include, for example, digital signatures and cryptographic hashes. Protection of system backup information while in transit is beyond the scope of this requirement. Information system backups reflect the requirements in contingency plans as well as other company requirements for backing up information.

Where to Look:

- contingency planning policy
- procedures addressing information system backup
- contingency plan
- backup storage location(s)
- information system backup logs or records
- other relevant documents or records

Who to Talk to:

- employees with information system backup responsibilities
- employees with information security responsibilities

Perform Test On:

- processes for conducting information system backups
- automated mechanisms supporting and/or implementing information system backups

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

Personnel Security: SP 800-171 Security Family 3.9

Users play a vital role in protecting a system as many important issues in information security involve users, designers, implementers, and managers. How these individuals interact with the system and the level of access they need to do their jobs can also impact the system's security posture. Almost no system can be secured without properly addressing these aspects of personnel security. Personnel security seeks to minimize the risk that staff (permanent, temporary, or contractor) pose to company assets through the malicious use or exploitation of their legitimate access to the company's resources. A company's status and reputation can be damaged by the actions of its employees. Employees may have access to extremely sensitive, or proprietary information, the disclosure of which can destroy an organization's reputation or cripple it financially. Companies should be vigilant when recruiting and hiring new employees, as well as when an employee transfers or is terminated. The sensitive nature and value of company assets requires in-depth personnel security measures. Examples of personnel requirement include: personnel screening, personnel termination, personnel transfer, access agreements, and personnel sanctions. Companies should ensure that individuals occupying positions of responsibility within the company (including third-party service providers) are trustworthy and meet established security criteria for those positions, ensure that company information and systems are protected during and after personnel actions such as terminations and transfers, and employ formal sanctions for personnel failing to comply with company security policies and procedures.

The following security requirements fall under the Personnel Security family.

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.9.1 Screen individuals prior to authorizing access to information systems containing CUI.

Are individuals requiring access screened before access is granted?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

Personnel screening and rescreening activities reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance.

Companies may define different rescreening conditions and frequencies for personnel accessing information systems based on types of information processed, stored, or transmitted by the systems.

Where to Look:

- personnel security policy
- procedures addressing personnel screening
- procedures addressing personnel termination
- procedures addressing personnel transfer
- records of personnel transfer actions
- list of information system and facility access authorizations
- records of personnel termination actions
- list of information system accounts
- records of terminated or revoked authenticators/credentials
- records of exit
- records of screened personnel
- security plan
- other relevant documents or records

Who to Talk to:

- employees with personnel security responsibilities
- employees with account management responsibilities
- employees with account management responsibilities
- system/network administrators
- employees with information security responsibilities

Perform Test On:

- processes for personnel screening
- processes for personnel termination
- automated mechanisms supporting and/ or implementing personnel termination notifications automated mechanisms for

  disabling information system access/ revoking authenticators

  processes for personnel transfer
- automated mechanisms supporting and/ or implementing personnel transfer notifications
- automated mechanisms for disabling information system access/revoking authenticators

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.9.2 Ensure that CUI and information systems containing CUI are protected during and after personnel actions such as terminations and transfers.

Does the company disable information system access prior to employee termination or transfer?

Yes No Partially Does Not Apply Alternative Approach

Does the company revoke authenticators/ credentials associated with the employee upon termination or transfer within a certain timeframe? (e.g., 24 hours)

Yes No Partially Does Not Apply Alternative Approach

Does the company retrieve all company information system-related property from the terminated or transferred employee within a certain timeframe? (e.g., 24 hours)

Yes No Partially Does Not Apply Alternative Approach

Does the company retain access to company information and information systems formerly controlled by the terminated or transferred employee within a certain timeframe? (e.g., 24 hours)

Yes No Partially Does Not Apply Alternative Approach

Does the company notify the information security office and data owner of the change in authorization within a certain timeframe? (e.g., 24 hours)

Yes No Partially Does Not Apply Alternative Approach

Are electronic and physical access permissions reviewed when employees are reassigned or transferred?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

This requirement applies when reassignments or transfers of individuals are permanent or of such extended durations as to make the actions warranted. Companies define actions appropriate for the types of reassignments or transfers, whether permanent or extended. Actions that may be required for personnel transfers or reassignments to other positions within companies include returning old and issuing new keys, identification cards, and building passes, closing information system accounts and establishing new accounts, changing information system access authorizations (i.e., privileges) and providing for access to official records to which employees had access at previous work locations and in previous information system accounts.

Where to Look:

- personnel security policy
- procedures addressing personnel screening
- procedures addressing personnel termination
- procedures addressing personnel transfer
- records of personnel transfer
- actions list of information system and facility access authorizations
- records of personnel termination actions
- list of information system accounts
- records of terminated or revoked authenticators/credentials
- records of exit
- records of screened personnel
- security plan
- other relevant documents or records

Who to Talk to:

- employees with personnel security responsibilities
- employees with account management responsibilities
- system/network administrators
- employees with information security responsibilities

Perform Test On:

- processes for personnel screening
- processes for personnel termination
- automated mechanisms supporting and/or implementing personnel termination notifications
- automated mechanisms for disabling information system access/revoking authenticators
- processes for personnel transfer
- automated mechanisms supporting and/or implementing personnel transfer notifications
- automated mechanisms for disabling information system access/revoking authenticators

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

Physical Protection: SP 800-171 Security Family 3.10

The term physical and environmental security refers to measures taken to protect systems, buildings, and related supporting infrastructure against threats associated with their physical environment. Physical and environmental requirements cover three broad areas:

1. The physical facility is typically the building, other structure, or vehicle housing the system and network components. Systems can be characterized, based upon their operating location, as static, mobile, or portable. Static systems are installed in structures at fixed locations. Mobile systems are installed in vehicles that perform the function of a structure, but not at a fixed location. Portable systems may be operated in a wide variety of locations, including buildings, vehicles, or in the open. The physical characteristics of these structures and vehicles determine the level of physical threats such as fire, roof leaks, or unauthorized access.
2. The facility's general geographic operating location determines the characteristics of natural threats, which include earthquakes and flooding; man-made threats such as burglary, civil disorders, or interception of transmissions and emanations; and damaging nearby activities, including toxic chemical spills, explosions, fires, and electromagnetic interference from emitters (e.g., radars).
3. Supporting facilities are those services (both technical and human) that maintain the operation of the system. The system's operation usually depends on supporting facilities such as electric power, heating and air conditioning, and telecommunications. The failure or substandard performance of these facilities may interrupt operation of the system and cause physical damage to system hardware or stored data.

Examples of physical and environmental requirements include: physical access authorizations, physical access control, monitoring physical access, emergency shutoff, emergency power, emergency lighting, alternate work site, information leakage, and asset monitoring and tracking. Companies should limit physical access to systems, equipment, and the respective operating environments to authorized individuals, protect the physical plant and support infrastructure for systems, provide supporting utilities for systems, protect systems against environmental hazards, and provide appropriate environmental controls in facilities containing systems.

The following security requirements fall under the Physical Protection family.

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.10.1 Limit physical access to company information systems, equipment, and the respective operating environments to authorized individuals.

Has the facility/building manager designated building areas as "sensitive" and designed physical security protections (including guards, locks, cameras, card readers, etc.) to limit physical access to the area to only authorized employees?

Yes No Partially Does Not Apply Alternative Approach

Are output devices such as printers placed in areas where their use does not expose data to unauthorized individuals?

Yes No Partially Does Not Apply Alternative Approach

Are lists of personnel with authorized access developed and maintained, and are appropriate authorization credentials issued?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

This requirement applies to company employees and visitors. Individuals (e.g., employees, contractors, and others) with permanent physical access authorization credentials are not considered visitors.

Authorization credentials include, for example, badges, identification cards, and smart cards. Organizations determine the strength of authorization credentials needed (including level of forgery-proof badges, smart cards, or identification cards). This requirement only applies to areas within facilities that have not been designated as publicly accessible.

The purpose of this requirement is simply to protect the information system/equipment by limiting physical access to the information system equipment to authorized organizational personnel (e.g., employees).

Where to Look:

- physical and environmental protection policy
- procedures addressing physical access authorizations
- procedures addressing access control for display medium
- procedures addressing physical access monitoring
- physical access logs or records
- physical access monitoring records
- physical access log reviews
- facility layout of information system components
- actual displays from information system components
- security plan
- authorized personnel access list
- authorization credentials
- physical access list reviews
- physical access termination records and associated documentation
- other relevant documents or records

Who to Talk to:

- employees with physical access authorization responsibilities
- employees with physical access to information system facility
- employees with physical access control responsibilities
- employees with physical access monitoring responsibilities
- employees with incident response responsibilities
- employees with information security responsibilities

Perform Test On:

- processes for physical access authorizations
- automated mechanisms supporting and/or implementing physical access authorizations
- processes for access control to output devices
- automated mechanisms supporting and/or implementing access control to output devices
- processes for monitoring physical access
- automated mechanisms supporting and/or implementing physical access monitoring
- automated mechanisms supporting and/or implementing reviewing of physical access logs

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.10.2 Protect and monitor the physical facility and support infrastructure for those information systems.

Has the facility/building manager reviewed the location and type of physical security in use (including guards, locks, card readers, etc.) and evaluated its suitability for the company's needs?

Yes No Partially Does Not Apply Alternative Approach

Is physical access monitored to detect and respond to physical security incidents?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

Company incident response capabilities include investigations of and responses to detected physical security incidents. Security incidents include, for example, apparent security violations or suspicious physical access activities. Suspicious physical access activities include accesses outside of normal work hours, repeated accesses to areas not normally accessed, accesses for unusual lengths of time, and out-of-sequence accesses.

Where to Look:

- physical and environmental protection policy
- procedures addressing physical access authorizations
- procedures addressing access control for display medium
- procedures addressing physical access monitoring
- physical access logs or records
- physical access monitoring records
- physical access log reviews
- facility layout of information system components
- actual displays from information system components
- security plan
- authorized personnel access list
- authorization credentials
- physical access list reviews
- physical access termination records and associated documentation
- other relevant documents or records

Who to Talk to:

- employees with physical access authorization responsibilities
- employees with physical access to information system facility
- employees with physical access control responsibilities
- employees with physical access monitoring responsibilities
- employees with incident response responsibilities
- employees with information security responsibilities

Perform Test On:

- processes for physical access authorizations
- automated mechanisms supporting and/or implementing physical access authorizations
- processes for access control to output devices
- automated mechanisms supporting and/or implementing access control to output devices
- processes for monitoring physical access
- automated mechanisms supporting and/or implementing physical access monitoring
- automated mechanisms supporting and/or implementing reviewing of physical access logs

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.10.3 Escort visitors and monitor visitor activity.

Are all visitors to sensitive areas always escorted by an authorized employee?

Yes No Partially Does Not Apply Alternative Approach

Are visitors escorted and monitored as required in security policies and procedures?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

Visitor access records include names and organizations of persons visiting, visitor signatures, forms of identification, dates of access, entry and departure times, purposes of visits, and names and organizations of persons visited. Visitor access records are not required for publicly accessible areas.

Where to Look:

- physical and environmental protection policy
- procedures addressing physical access control
- security plan
- physical access control logs or records
- inventory records of physical access control devices
- information system entry and exit points
- records of key and lock combination changes
- storage locations for physical access control devices
- physical access control devices
- list of security safeguards controlling access to designated publicly accessible areas within facility
- other relevant documents or records

Who to Talk to:

- employees with physical access control responsibilities
- employees with information security responsibilities

Perform Test On:

- processes for physical access control
- automated mechanisms supporting and/or implementing physical access control
- physical access control devices

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.10.4 Maintain audit logs of physical access.

Are logs of physical access to sensitive areas maintained per retention policies? (This includes authorized access as well as visitor access.)

Yes No Partially Does Not Apply Alternative Approach

Are visitor access records retained for as long as required by approved policy?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

This requirement applies to company employees and visitors. Individuals (employees with physical access control responsibilities, employees, contractors, and others) with permanent physical access authorization credentials are not considered visitors. Companies determine the types of facility guards needed including, for example, professional physical security staff or other personnel such as administrative staff or information system users. Physical access devices include keys, locks, combinations, and card readers. Safeguards for publicly accessible areas within company facilities include cameras, monitoring by guards, and isolating selected information systems and/or system components in secured areas.

Companies have flexibility in the types of audit logs they employ. Audit logs can be procedural, implemented by employees with physical access control responsibilities, a written log of individuals accessing the facility and when such access occurred), automated (employees with physical access control responsibilities, capturing ID provided by a smart card or badge), or some combination thereof. Physical access points can include facility access points, interior access points to information systems and/or components requiring supplemental access controls, or both.

Components of company information systems (e.g., employees with physical access control responsibilities, workstations, terminals) may be in areas designated as publicly accessible with organizations safeguarding access to such devices.

Where to Look:

- physical and environmental protection policy
- procedures addressing physical access control
- security plan
- physical access control logs or records
- inventory records of physical access control devices
- information system entry and exit points
- records of key and lock combination changes
- storage locations for physical access control devices
- physical access control devices
- list of security safeguards controlling access to designated publicly accessible areas within facility
- other relevant documents or records

Who to Talk to:

- employees with physical access control responsibilities
- employees with information security responsibilities

Perform Test On:

- processes for physical access control
- automated mechanisms supporting and/or implementing physical access control
- physical access control devices

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.10.5 Control and manage physical access devices.

Are physical access devices (such as card readers, proximity readers, and locks) maintained and operated per the manufacturer recommendations?

Yes No Partially Does Not Apply Alternative Approach

Are these devices updated with any changed access control information necessary to prevent unauthorized access?

Yes No Partially Does Not Apply Alternative Approach

Does the facility/building manager review the location and type of each physical access device and evaluate its suitability for the company's needs?

Yes No Partially Does Not Apply Alternative Approach

Are keys, combinations, and other physical access devices secured?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

Organizations determine the types of facility guards needed including, for example, professional physical security staff or other personnel such as administrative staff or information system users. Physical access devices include keys, locks, combinations, and card readers. Safeguards for publicly accessible areas within company facilities include cameras, monitoring by guards, and isolating selected information systems and/or system components in secured areas.

Companies have flexibility in the types of audit logs employed. Audit logs can be procedural (e.g., a written log of individuals accessing the facility and when such access occurred), automated (e.g., capturing ID provided by a smart card or badge), or some combination thereof. Physical access points can include facility access points, interior access points to information systems and/or components requiring supplemental access controls, or both. Components of company information systems (e.g., workstations, terminals) may be in areas designated as publicly accessible with organizations safeguarding access to such devices.

Where to Look:

- physical and environmental protection policy
- procedures addressing physical access control
- security plan
- physical access control logs or records
- inventory records of physical access control devices
- information system entry and exit points
- records of key and lock combination changes
- storage locations for physical access control devices
- physical access control devices
- list of security safeguards controlling access to designated publicly accessible areas within facility
- other relevant documents or records

Who to Talk to:

- employees with physical access control responsibilities
- employees with information security responsibilities

Perform Test On:

- processes for physical access control
- automated mechanisms supporting and/or implementing physical access control
- physical access control devices

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.10.6 Enforce safeguarding measures for CUI at alternate work sites (e.g., telework sites).

Do all alternate sites where CUI data is stored or processed meet the same physical security requirements as the main site?

Yes No Partially Does Not Apply Alternative Approach

Does the alternate processing site provide information security measures equivalent to those of the primary site?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

Alternate work sites may include, for example, government facilities or private residences of employees. While commonly distinct from alternative processing sites, alternate work sites may provide readily available alternate locations as part of contingency operations. Companies may define different sets of security requirements for specific alternate work sites or types of sites depending on the work-related activities conducted at those sites. This requirement supports the contingency planning activities of the company.

This requirement simply means that if you have alternate work sites that will be used to store, process, or transmit CUI, that the same requirements apply (i.e., there is no difference in requirements between the primary and alternate work sites), although different methods may be used to meet the requirements at the alternate site.

Where to Look:

- physical and environmental protection policy
- procedures addressing alternate work sites for employees
- security plan
- list of security requirements required for alternate work sites
- assessments of security requirements at alternate work sites
- other relevant documents or records

Who to Talk to:

- employees approving use of alternate work sites
- employees using alternate work sites
- employees assessing controls at alternate work sites
- employees with information security responsibilities

Perform Test On:

- processes for security at alternate work sites
- automated mechanisms supporting alternate work sites
- security requirements employed at alternate work sites
- means of communications between personnel at alternate work sites and security personnel

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

Risk Assessment: SP 800-171 Security Family 3.11

Companies are dependent upon information technology and associated systems. While the increasing number of information technology products used in various companies and industries can be beneficial, in some instances they may also introduce serious threats that can adversely affect a company's systems by exploiting both known and unknown vulnerabilities. The exploitation of vulnerabilities in company systems can compromise the confidentiality, integrity, or availability of the information being processed, stored, or transmitted by those systems. Performing a risk assessment is one of four components of risk management. Risk assessments identify and prioritize risks to company operations, assets, employees, and other organizations that may result from the operation of a system. Risk assessments inform company decision makers and support risk responses by identifying: relevant threats to organizations or threats directed through organizations against other organizations, vulnerabilities both internal and external to organizations, impact (i.e., harm) to the company that may occur given the potential for threats exploiting vulnerabilities, and the likelihood that harm will occur.

Examples of risk assessment requirements include: security categorization, risk assessment, vulnerability scanning, and technical surveillance countermeasures survey. Companies should periodically assess the risk to operations (e.g., mission, functions, image, reputation), assets, and employees, which may result from the operation of company systems and the associated processing, storage, or transmission of company information.

The following security requirements fall under the Risk Assessment family.

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.11.1 Periodically assess the risk to company operations (including mission, functions, image, or reputation), company assets, and individuals, resulting from the operation of company information systems and the associated processing, storage, or transmission of CUI.

Does the company have a risk management policy?

Yes No Partially Does Not Apply Alternative Approach

Have an initial and periodic risk assessments been conducted?

Yes No Partially Does Not Apply Alternative Approach

Are changes in use or infrastructure documented and assessed?

Yes No Partially Does Not Apply Alternative Approach

Is the risk assessment viewed as a living document and incorporated into the larger risk management for the system?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

Risk assessments play a critical role in the development and implementation of effective information security programs and help companies address a range of security-related issues from advanced persistent threats to supply chain concerns. The results of risk assessments are used to develop specific courses of action that can provide effective response measures to the identified risks as part of a broad-based risk management process.

There is no defined requirement, methodology, or period for the assessments, nor is a report required. These are dependent on the organization, its mission, changes to its systems and environment. This is a periodic assessment of how you operate to insure you understand your risk, which can change over time. Any changes resulting from the assessment would be reflected in implementing plans of action and in the system security plan per NIST SP 800-171 requirements 3.12.2 and 3.12.4.

Additional information on conducting risk assessments can be found in NIST 800-30 Rev 1 “Guide for Conducting Risk Assessments”

http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

Additional information

Where to Look:

- risk assessment policy
- security planning policy and procedures
- procedures addressing company assessments of risk
- security plan
- risk assessment
- risk assessment results
- risk assessment reviews
- risk assessment updates
- other relevant documents or records

Who to Talk to:

- employees with risk assessment responsibilities
- employees with information security responsibilities

Perform Test On:

- processes for risk assessment
- automated mechanisms supporting and/ or for conducting, documenting, reviewing, disseminating, and updating the risk assessment

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.11.2 Scan for vulnerabilities in the information system and applications periodically and when new vulnerabilities affecting the system are identified.

Is vulnerability scanning performed?

Yes No Partially Does Not Apply Alternative Approach

Are systems periodically scanned for common and new vulnerabilities?

Yes No Partially Does Not Apply Alternative Approach

Are previously undocumented vulnerabilities risk assessed and documented?

Yes No Partially Does Not Apply Alternative Approach

Are reports regarding the scans made available to system owners and company management in a timely manner?

Yes No Partially Does Not Apply Alternative Approach

Are vulnerability scans performed on a defined frequency or randomly in accordance with company policy?

Yes No Partially Does Not Apply Alternative Approach

Is the list of scanned system vulnerabilities updated on a defined frequency or when new vulnerabilities are identified and reported?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

Vulnerability scanning identifies hosts and host attributes (e.g., operating systems, applications, open ports), but it also attempts to identify vulnerabilities rather than relying on human interpretation of the scanning results. Many vulnerability scanners are equipped to accept results from network discovery and network port and service identification, which reduces the amount of work needed for vulnerability scanning.

Also, some scanners can perform their own network discovery and network port and service identification. Vulnerability scanning can help identify outdated software versions, missing patches, and misconfigurations, and validate compliance with or deviations from an organization's security policy. This is done by identifying the operating systems and major software applications running on the hosts and matching them with information on known vulnerabilities stored in the scanners' vulnerability databases.

Vulnerability scanners can: check compliance with host application usage and security policies; provide information on targets for penetration testing; and provide information on how to mitigate discovered vulnerabilities.

Where to Look:

- risk assessment policy
- procedures addressing vulnerability scanning records
- risk assessment
- security plan
- information system design documentation
- information system configuration settings and associated documentation
- list of information system components for vulnerability scanning
- personnel access authorization list
- authorization credentials
- access authorization
- security assessment report
- vulnerability scanning tools and associated configuration documentation
- vulnerability scanning results
- patch and vulnerability management records
- other relevant documents or records

Who to Talk to:

- employees with risk assessment, security control assessment and vulnerability scanning responsibilities
- employees with vulnerability scan analysis responsibilities
- employees with vulnerability remediation responsibilities
- personnel with vulnerability scanning responsibilities system/network administrators
- employees responsible for access control to the information system
- employees responsible for configuration management of the information system
- system developers
- employees with information security

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

responsibilities

- system/network administrators

Perform Test On:

- processes for vulnerability scanning, analysis, remediation, and information sharing
- automated mechanisms supporting and/or implementing vulnerability scanning, analysis, remediation, and information sharing
- processes for vulnerability scanning
- processes for access control
- automated mechanisms supporting and/or implementing access control
- automated mechanisms/tools supporting and/ or implementing vulnerability scanning

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.11.3 *Remediate vulnerabilities in accordance with assessments of risk.*

Do system owners and company managers upon recognition of any vulnerability provide an action plan for remediation, acceptance, avoidance, or transference of the vulnerability risk?

Yes No Partially Does Not Apply Alternative Approach

Does the plan include a reasonable time frame for implementation?

Yes No Partially Does Not Apply Alternative Approach

Are all high vulnerabilities prioritized?

Yes No Partially Does Not Apply Alternative Approach

Does the Plan of Action call out remedial security actions to mitigate risk to company operations, assets, employee,s and other organizations?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

Clearly defined authorization boundaries are a prerequisite for effective risk assessments. Risk assessments consider threats, vulnerabilities, likelihood, and impact to company operations and assets, employees, and other organizations based on the operation and use of information systems. Risk assessments also consider risk from external parties (e.g., service providers, contractors operating information systems on behalf of the company, individuals accessing company information systems, outsourcing entities).

Risk assessments (either formal or informal) can be conducted at all three tiers in the risk management hierarchy (i.e., organization level, mission/business process level, or information system level) and at any phase in the system development life cycle.

Where to Look:

- risk assessment policy
- procedures addressing vulnerability scanning
- risk assessment
- security plan
- security assessment report
- vulnerability scanning tools and associated configuration documentation
- vulnerability scanning results
- patch and vulnerability management records
- other relevant documents or records

Who to Talk to:

- employees with risk assessment, security requirement assessment and vulnerability scanning responsibilities
- employees with vulnerability scan analysis responsibilities
- employees with vulnerability remediation responsibilities
- employees with information security responsibilities
- system/network administrators

Perform Test On:

- processes for vulnerability scanning, analysis, remediation, and information sharing
- automated mechanisms supporting and/or implementing vulnerability scanning, analysis, remediation, and information sharing

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

Security Assessment: SP 800-171 Security Family 3.12

A security requirement assessment is the testing and/or evaluation of the management, operational, and technical security requirements on a system to determine the extent to which the requirements are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. The assessment also helps determine if the implemented requirements are the most effective and cost-efficient solution for the function they are intended to serve. Assessment of the security requirements is done on a continuous basis to support a near real-time analysis of the organization's current security posture. Following a complete and thorough security requirement assessment, the company makes the decision to authorize the system to operate (for a new system) or to continue to operate. Examples of security assessment and authorization requirements include: security assessments, system interconnections, plans of action, continuous monitoring, and system security plans. Companies should periodically assess the security requirements in company systems to determine if the requirements are effective in their application, develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in company systems, authorize the operation of company systems and any associated system connections, and monitor security requirements on an ongoing basis to ensure the continued effectiveness of the requirements, and document these actions in the System Security Plan.

The following security requirements fall under the Security Assessment family.

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.12.1 Periodically assess the security controls in company information systems to determine if the controls are effective in their application.

Has a periodic (e.g., annual) security assessment been conducted to ensure that security controls are implemented correctly and meet the security requirements?

Yes No Partially Does Not Apply Alternative Approach

Does the assessment scope include all information systems and networks, including all security requirements and procedures necessary to meet the compliance requirements of the environment?

Yes No Partially Does Not Apply Alternative Approach

Does the assessment include, but is not limited to, vulnerability scanning, penetration testing, security control testing and reviews, configuration testing and reviews, log reviews, and talking with company employees?

Yes No Partially Does Not Apply Alternative Approach

Is the assessment conducted by company employees?

Yes No Partially Does Not Apply Alternative Approach

Is the assessment conducted by an independent security auditor/consultant?

Yes No Partially Does Not Apply Alternative Approach

Is a final written assessment report and findings provided to company management after the assessment?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

To satisfy periodic (e.g., annual) assessment requirements, companies can use assessment results from the initial or ongoing information system authorizations, continuous monitoring, or system development life cycle activities.

Companies should ensure that security assessment results are current, relevant to the determination of security requirement effectiveness, and obtained with the appropriate level of assessor independence. Existing security requirement assessment results can be reused to the extent that the results are still valid and can also be supplemented with additional assessments as needed. Companies should establish the frequency for ongoing security requirement assessments in accordance with company continuous monitoring strategies. Information Assurance Vulnerability Alerts provide useful examples of vulnerability mitigation procedure. Assessments should be performed at least annually. External audits (e.g., audits by external entities such as regulatory agencies) are outside the scope of this requirement.

The company should define for itself when requirements are assessed, which may be based on a timeframe determined by its needs and/or events, such as a change to the system or its environment.

Where to Look:

- security assessment and authorization policy
- procedures addressing security assessment planning
- procedures addressing security assessments
- procedures addressing plan of action
- procedures addressing continuous monitoring of information system security requirements
- procedures addressing configuration management
- plan of action
- information system monitoring records
- configuration management records
- security impact analyses
- status reports
- security plan
- security assessment report
- security assessment evidence
- plan of action
- security assessment plan
- other relevant documents or records

Who to Talk to:

- employees with security assessment

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

responsibilities

- employees with plan of action development and implementation responsibilities
- employees with continuous monitoring responsibilities
- employees with information security responsibilities

Perform Test On:

- automated mechanisms supporting security assessment, security assessment plan development, and/or security assessment reporting
- automated mechanisms for developing, implementing, and maintaining plan of action
- mechanisms implementing continuous monitoring

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in company information systems.

Is there an action plan to remediate identified weaknesses or deficiencies?

Yes No Partially Does Not Apply Alternative Approach

Is the action plan maintained as remediation is performed?

Yes No Partially Does Not Apply Alternative Approach

Does the action plan designate remediation dates and milestones for each item?

Yes No Partially Does Not Apply Alternative Approach

Are deficiencies and weaknesses identified in security requirements assessments added to the action plan within a specified timeframe (e.g., 30 days) of the findings being reported?

Yes No Partially Does Not Apply Alternative Approach

Additional information

Plans of Action should address how and when any unimplemented security requirements or partially met security requirements will be addressed, how any planned improvements will be implemented, and how and when deficiencies will be corrected and how they will reduce or eliminate vulnerabilities in the system**.** Companies can document the system security plan and plans of action as separate or combined documents in any chosen format

Where to Look:

- security assessment and authorization policy
- procedures addressing security assessment planning
- procedures addressing security assessments
- procedures addressing plan of action
- procedures addressing continuous monitoring of information system security requirements
- procedures addressing configuration management
- information system monitoring records
- configuration management records,
- security impact analyses
- status reports
- security assessment report
- security assessment evidence
- plan of action
- security assessment plan
- other relevant documents or records

Who to Talk to:

- employees with security assessment responsibilities
- employees with plan of action development and implementation responsibilities employees with continuous monitoring responsibilities
- employees with information security responsibilities
- system/network administrators

Perform Test On:

- automated mechanisms supporting security assessment, security assessment plan development, and/or security assessment reporting
- automated mechanisms for developing, implementing, and maintaining plan of action
- mechanisms implementing continuous monitoring

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.12.3 Monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.

Are continuous monitoring tools deployed for front internet facing systems (computers with IP addresses that can be reached from the internet) or those used to store or transmit sensitive data?

Yes No Partially Does Not Apply Alternative Approach

At a minimum, are these systems monitored for privileged access, permission changes, kernel modifications, and binary changes against a control and system baseline?

Yes No Partially Does Not Apply Alternative Approach

Are continuous monitoring reports and alerts reviewed frequently (e.g., daily)?

Yes No Partially Does Not Apply Alternative Approach

Are unauthorized changes or unauthorized access reported to company management, and information system owner within a certain timeframe (e.g., 24 hours) of it being discovered?

Yes No Partially Does Not Apply Alternative Approach

Is there an assessor or assessment team to monitor the security requirement in the system on an ongoing basis?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

Companies can maximize the value of assessments of security requirements during the continuous monitoring process by requiring that such assessments be conducted by assessors or assessment teams with appropriate levels of independence based on continuous monitoring strategies. Assessor independence provides a degree of impartiality to the monitoring process.

There is no defined period for security requirement assessments. The company should define for itself when requirements are assessed, which may be based on a timeframe determined by its needs and/ or events, such as a change to the system or its environment.

There is no prescribed format or level of specificity for a system security plan (see 3.12.4 System Security Plan), and DOD Contracting Officers/Requiring Activities should not prescribe a format or level of specificity. Per Chapter 3 of NIST SP 800-171, rev 1, "Organizations can document the system security plan and plan of action as separate or combined documents and in any chosen format."

The complete system security plan can be quite sensitive and typically DOD does not need the description of system boundaries and operational environment (or other sensitive information that the company may have included in the system security plan to make it operationally useful for their purposes) to demonstrate the organization's implementation or planned implementation of the NIST SP 800-171 security requirements.

Accordingly, the requiring activity/contracting officer should not require in the solicitation that the actual system security plan be submitted, but rather an extract that describes how the individual security requirements are implemented, and any associated plans of action to implement security requirements not yet met. A company should tailor its submission, or extract of the system security plan, to provide only the information required by the solicitation, and avoid including sensitive information that is not required.

The requiring activity may specify in the solicitation, however, that the contractor must provide information in the technical proposal in a particular format and level of detail. This should NOT be interpreted as prescribing a particular format or level of detail for a contractor's system security plan or plans of action.

Also in accordance with Chapter 3 of NIST SP 800-171, rev 1, "federal agencies may consider the submitted system security plans and plans of action as critical inputs to an overall risk management decision to process, store, or transmit CUI on a system hosted by a nonfederal organization." As such, they may determine that the risk is such that they will not pursue an agreement or contract with the organization.

Where to Look:

- security assessment and authorization policy
- procedures addressing security assessment planning
- procedures addressing security assessments
- procedures addressing plan of action
- procedures addressing continuous monitoring of information system security requirements
- procedures addressing configuration management
- security plan
- security assessment plan

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

- security assessment report
- security assessment evidence
- plan of action
- information system monitoring records
- configuration management records,
- security impact analyses
- status reports
- other relevant documents or records

Who to Talk to:

- employees with security assessment responsibilities
- employees with plan of action development and implementation responsibilities
- employees with continuous monitoring responsibilities
- employees with information security responsibilities
- system/network administrators

Perform Test On:

- automated mechanisms supporting security assessment, security assessment plan development, and/or security assessment reporting
- automated mechanisms for developing, implementing, and maintaining plan of action
- mechanisms implementing continuous monitoring

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.12.4 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.

Are system security plans consistent with the organization's enterprise architecture?

Yes No Partially Does Not Apply Alternative Approach

Does the system security plan explicitly define the authorization boundary for the system?

Yes No Partially Does Not Apply Alternative Approach

Does the system security plan describe the operational context of the system in terms of missions and business processes?

Yes No Partially Does Not Apply Alternative Approach

Does the system security plan describe the operational environment for the system?

Yes No Partially Does Not Apply Alternative Approach

Does the system security plan describe relationships with or connections to other systems?

Yes No Partially Does Not Apply Alternative Approach

Does the system security plan provide an overview of the security and privacy requirements for the system?

Yes No Partially Does Not Apply Alternative Approach

Does the system security plan describe the security requirements in place?

Yes No Partially Does Not Apply Alternative Approach

Does the system security plan include plans for meeting those requirements not yet in place?

Yes No Partially Does Not Apply Alternative Approach

Is the system security plan reviewed and approved by company management prior to plan implementation?

Yes No Partially Does Not Apply Alternative Approach

Are copies of the system security plan distribute to relevant company employees?

Yes No Partially Does Not Apply Alternative Approach

Are changes to the system security plan communicated to relevant company employees?

Yes No Partially Does Not Apply Alternative Approach

Does the company periodically review the system security plan within a certain timeframe? (e.g., annually)

Yes No Partially Does Not Apply Alternative Approach

Does the company update the system security plan to address changes to the system, environment of operation or problems identified during plan implementation or security assessments?

Yes No Partially Does Not Apply Alternative Approach

Does the company protect the system security plan from unauthorized disclosure and modification?

Yes No Partially Does Not Apply Alternative Approach

Does the company plan and coordinate security-related activities affecting the system before conducting any such activities?

Yes No Partially Does Not Apply Alternative Approach

Are security-related activities planned to reduce the impact on other company entities?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

There is no prescribed format or specified level of detail for system security plans. However, companies must ensure that the required information in 3.12.4 is appropriately conveyed in those plans.

Some systems, including specialized systems (e.g., industrial/process control systems, Computer Numerical Control (CNC) machines), may have restrictions or limitations on the application of certain security requirements. To accommodate such issues, the system security plan should be used to describe any enduring exceptions to the security requirements. Individual, isolated, or temporary deficiencies should be managed though plans of action.

System security plans describe how the company meets the security requirements but do not provide detailed, technical descriptions of the specific design or implementation. System security plans contain sufficient information to enable a design and implementation that is unambiguously compliant with the intent of the plans and subsequent determinations of risk to company operations and assets, employees, and other organizations, if the plan is implemented as intended.

System security plans need not be single documents. The plans can be a collection of various documents including documents that already exist within the company. Effective systems security plans make extensive use of references to policies, procedures,

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

and additional documents including, for example, design and implementation specifications where more detailed information can be obtained. This reduces the documentation associated with security programs and maintains the security-related information in other established management and operational areas including, for example, enterprise architecture, system development life cycle, systems engineering, and acquisition. System security plans do not contain detailed contingency plan or incident response plan information but instead provide sufficient information to define what needs to be accomplished by those plans.

Where to Look:

- security planning policy
- procedures addressing security plan development and implementation
- procedures addressing security plan reviews and updates
- enterprise architecture documentation
- security plan for the information system
- records of security plan reviews and updates
- other relevant documents or records

Who to Talk to:

- employees with security planning and plan implementation responsibilities
- employees with information security responsibilities

Perform Test On:

- automated mechanisms supporting system security plan development
- automated mechanisms for developing, implementing, and maintaining system security plans

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

Systems and Communications Protection: SP 800-171 Security Family 3.13

System and communications protection requirements provide an array of safeguards for the system. Some of the requirements in this family address the confidentiality information at rest and in transit. The protection of confidentiality can be provided by these requirements through physical or logical means. For example, a company can provide physical protection by segregating certain functions to separate servers, each having its own set of IP addresses. Companies can better safeguard their information by separating user functionality and system management functionality. Providing this type of protection prevents the presentation of system management-related functionality on an interface for non-privileged users. System and communications protection also establishes boundaries that restrict access to publicly accessible information within a system. Using boundary protections, a company can monitor and control communications at external boundaries as well as key internal boundaries within the system.

Examples of system and communication protection requirements include: application partitioning, denial of service protection, boundary protection, trusted path, mobile code, session authenticity, thin nodes, honeypots, transmission confidentiality and integrity, operations security, protection of information at rest and in transit, and usage restrictions. Companies should:

- monitor, control, and protect company communications (i.e., information transmitted or received by company systems) at the external boundaries and key internal boundaries of the systems and
- employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within company systems.

The following security requirements fall under the Systems and Communication Protection family.

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.13.1 *Monitor, control, and protect company communications (i.e., information transmitted or received by organization information systems) at the external boundaries and key internal boundaries of the information systems.*

Has the company identified network communications boundaries?

Yes No Partially Does Not Apply Alternative Approach

Does the system monitor and manage communications at the system boundary and at key internal boundaries within the system?

Yes No Partially Does Not Apply Alternative Approach

Do policies for managed interfaces such as gateways, routers, firewalls, VPNs, and company DMZs restrict external web traffic to only designated servers exist?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

Portable media refers to storing and playing digital media such as audio, images and video files. The data is typically stored on a CD, DVD, flash memory, microdrive, or hard drive located on portable devices, and therefore can easily be taken outside of system boundaries.

Boundary protection refers to the monitoring and control of communications at the external boundary of an information system. Boundary protection is used to prevent and detect malicious and other unauthorized communications. Boundary protection devices may include gateways, routers, firewalls, guards, and encrypted tunnels.

Where to Look:

- system and communications protection policy
- procedures addressing boundary protection
- procedures addressing security engineering principles used in the specification, design, development, implementation, and modification of the information system
- information security requirements and specifications
- list of key internal boundaries of the information system
- information system design documentation
- boundary protection hardware and software
- information system configuration settings and associated documentation
- enterprise security architecture documentation
- information system audit records
- other relevant documents or records

Who to Talk to:

- system/network administrators
- employees with responsibility for determining information system security requirements
- employees with information system specification, design, development, implementation, and modification responsibilities
- information system developers
- employees with boundary protection responsibilities
- employees with information security responsibilities

Perform Test On:

- automated mechanisms implementing boundary protection capability
- automated mechanisms supporting the application of security engineering principles in information system specification, design, development, implementation, and modification

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.13.2 *Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within company information systems.*

Are the company's information security policies (including architectural design, software development, and system engineering principles) designed to promote information security?

Yes No Partially Does Not Apply Alternative Approach

Are the policies adequate to meet the needs of the company?

Yes No Partially Does Not Apply Alternative Approach

Are system security engineering principles applied in the specification, design, development, and implementation of the system?

Yes No Partially Does Not Apply Alternative Approach

Is the system managed using a system development life-cycle methodology that includes security considerations?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

Companies should apply security engineering principles primarily to new development of information systems or systems undergoing major upgrades. For legacy systems, organizations apply security engineering principles to system upgrades and modifications to the extent feasible, given the current state of hardware, software, and firmware within those systems. Security engineering principles include:

- developing layered protections
- establishing sound security policy
- architecture, and controls as the foundation for design
- incorporating security requirements into the system development life cycle
- delineating physical and logical security boundaries
- ensuring that system developers are trained on how to build secure software
- tailoring security requirements to meet company and operational needs
- performing threat modeling to identify use cases, threat agents, attack vectors, and attack patterns as well as compensating controls and design patterns needed to mitigate risk and reducing risk to acceptable levels, enabling informed risk management decisions

Where to Look:

- system and communications protection policy
- system and services acquisition policy procedures addressing boundary protection
- procedures addressing security engineering principles used in the specification, design, development, implementation, and modification of the information system
- information security requirements and specifications for the information system
- list of key internal boundaries of the information system
- information system design documentation
- boundary protection hardware and software information
- system configuration settings and associated documentation
- enterprise security architecture documentation
- information system audit records
- other relevant documents or records

Who to Talk to:

- system/network administrators
- system developers
- employees with responsibility for determining information system security requirements
- employees with information system specification, design, development, implementation, and modification responsibilities
- employees with information security responsibilities

Perform Test On:

- automated mechanisms implementing boundary protection capability
- processes for applying security engineering principles in information system specification, design, development, implementation, and modification

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

- automated mechanisms supporting the application of security engineering principles in information system specification, design, development, implementation, and modification

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.13.3 *Separate user functionality from information system management functionality.*

Are physical or logical controls used to separate user functionality from system management-related functionality (e.g., to ensure that administration [e.g., privilege] options are not available to general users)?

Yes No Partially Does Not Apply Alternative Approach

Is user functionality separated from system management functionality?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

Information system management functionality includes, for example, functions necessary to administer databases, network components, workstations, or servers, and typically requires privileged user access. The separation of user functionality from information system management functionality is either physical or logical. Companies implement separation of system management-related functionality from user functionality by using different computers, different central processing units, different instances of operating systems, different network addresses, virtualization techniques, or combinations of these or other methods, as appropriate. This type of separation includes, for example, web administrative interfaces that use separate authentication methods for users of any other information system resources. Separation of system and user functionality may include isolating administrative interfaces on different domains and with additional access controls.

Where to Look:

- system and communications protection policy
- procedures addressing application partitioning
- information system design documentation
- information system configuration settings and associated documentation
- information system audit records
- other relevant documents or records

Who to Talk to:

- system/network administrators
- employees with information security responsibilities
- system developers

Perform Test On:

- separation of user functionality from information system management functionality

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.13.4 *Prevent unauthorized and unintended information transfer via shared system resources.*

Are requirements implemented to prevent object reuse and to protect residual information?

Yes No Partially Does Not Apply Alternative Approach

Does the system prevent unauthorized or unintended information transfer via shared system resources, e.g., register, main memory, secondary storage?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

This requirement prevents information, including encrypted representations of information, produced by the actions of prior users/roles (or the actions of processes acting on behalf of prior users/roles) from being available to any current users/roles (or current processes) that obtain access to shared system resources (e.g., registers, main memory, hard disks) after those resources have been released back to information systems.

The control of information in shared resources is also commonly referred to as object reuse and residual information protection. This requirement does not address information remanence which refers to residual representation of data that has been nominally erased or removed, covert channels (including storage and/or timing channels) where shared resources are manipulated to violate information flow restrictions, or components within information systems for which there are only single users/roles.

Where to Look:

- system and communications protection policy
- procedures addressing information protection in shared system resources
- information system design documentation
- information system configuration settings and associated documentation
- information system audit records
- other relevant documents or records

Who to Talk to:

- system/network administrators
- employees with information security responsibilities
- system developers

Perform Test On:

- automated mechanisms preventing unauthorized and unintended transfer of information via shared system

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.13.5 *Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.*

Does the company implement DMZs?

Yes No Partially Does Not Apply Alternative Approach

Are they adequate to meet the needs of the company?

Yes No Partially Does Not Apply Alternative Approach

Does the system monitor and manage communications at the system boundary and at key internal boundaries within the system?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

In cybersecurity, a demilitarized zone (DMZ), sometimes referred to as a perimeter network, is a physical or logical subnetwork that contains and exposes a company's external-facing services to an untrusted network, usually a larger network such as the internet. The purpose of a DMZ is to add an additional layer of security to a company's LAN, an external network node can access only what is exposed in the DMZ, and can be intensely managed and audited, while the rest of the company's network is firewalled.

Where to Look:

- system and communications protection policy
- system and services acquisition policy
- procedures addressing boundary protection
- procedures addressing security engineering principles used in the specification, design, development, implementation, and modification of the information system
- information system design documentation
- information security requirements and specifications
- list of key internal boundaries of the information system
- information system design documentation
- boundary protection hardware and software
- information system configuration settings and associated documentation
- enterprise security architecture
- information system audit records
- other relevant documents or records

Who to Talk to:

- system/network administrators
- employees with information security responsibilities
- system developer
- employees with boundary protection responsibilities
- employees with responsibility for determining information system security requirements
- employees with information system specification, design, development, implementation, and modification responsibilities
- information system developers
- employees with information security responsibilities

Perform Test On:

- automated mechanisms implementing boundary protection capability
- processes for applying security engineering principles in information system specification, design, development, implementation, and modification
- automated mechanisms supporting the application of security engineering principles in information system specification, design, development, implementation, and modification

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.13.6 Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).

Are all business need exceptions to network communications traffic (inbound/outbound) “deny all” policies documented?

Yes No Partially Does Not Apply Alternative Approach

Does the system deny network traffic by default and allow network traffic by exception?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

Firewalls and routers placed at the perimeter of the system should only allowed traffic that is permitted to flow through. A permit by exception policy is used to allow the use of authorized programs.

Where to Look:

- system and communications protection policy
- procedures addressing boundary protection
- information system design documentation
- information system configuration settings and associated documentation
- information system audit records
- other relevant documents or records

Who to Talk to:

- system/network administrators
- employees with information security responsibilities
- system developers
- employees with boundary protection responsibilities

Perform Test On:

- automated mechanisms implementing traffic management at managed interfaces

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.13.7 Prevent remote devices from simultaneously establishing non-remote connections with the information system and communicating via some other connection to resources in external networks.

Are controls in place to prevent split tunneling in remote devices, and to mandate VPN use when necessary for business functions?

Yes No Partially Does Not Apply Alternative Approach

Does the system prevent remote devices that have established connections (e.g., remote laptops) with the system from communicating outside that communications path with resources on uncontrolled/unauthorized networks?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

Split tunneling allows a mobile user to access dissimilar security domains like a public network (e.g., the internet) and a LAN or WAN at the same time, using the same or different network connections.

A VPN is a virtual network built on top of existing networks that can provide a secure communications mechanism for data and IP information transmitted between networks. A common example is a a tunnel that connects an employee's laptop to the company's network.

Where to Look:

- system and communications protection policy
- procedures addressing boundary protection
- information system design documentation
- information system hardware and software
- information system architecture
- information system configuration settings and associated documentation
- information system audit records
- other relevant documents or records

Who to Talk to:

- system/network administrators
- employees with information security responsibilities
- system developer
- employees with boundary protection responsibilities

Perform Test On:

- automated mechanisms implementing boundary protection capability
- automated mechanisms supporting/restricting non-remote connections

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.13.8 *Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.*

Are cryptographic mechanisms used to prevent unauthorized disclosure of information during transmission unless otherwise protected by alternative physical measures?

Yes No Partially Does Not Apply Alternative Approach

Are processes and automated mechanisms used to provide encryption of CUI during transmission?

Yes No Partially Does Not Apply Alternative Approach

Are all alternative physical safeguards used to provide confidentiality of CUI during transmission documented?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

Encrypting information for transmission protects information from unauthorized disclosure and modification. Cryptographic mechanisms implemented to protect information integrity include, for example, cryptographic hash functions which have common application in digital signatures, checksums, and message authentication codes. Alternative physical security safeguards include, for example, protected distribution systems.

The NIST SP 800-171 requirements for cryptography used to protect the confidentiality of CUI must use FIPS-validated cryptography, which means the cryptographic module must have been tested and validated to meet FIPS 140-1 or -2 requirements. Simply using an approved algorithm (e.g., FIPS 197 for AES) is not sufficient. The module (software and/or hardware) used to implement the algorithm must be separately validated under FIPS 140. When an application or device allows a choice (by selecting FIPS-mode or not), then the FIPS-mode has been validated under FIPS 140-2, but the other options (non-FIPS) allow certain operations that would not meet the FIPS requirements. More information is available at

http://csrc.nist.gov/groups/STM/cmvp/

When NIST SP 800-171 requires cryptography, it is to protect the confidentiality of CUI. Accordingly, FIPS-validated cryptography is required to protect CUI, typically when transmitted or stored outside the protected environment of the covered contractor information system (including wireless/remote access) if not separately protected (e.g., by a protected distribution system). FIPS-validated cryptography is required whenever the encryption is required to protect covered defense information in accordance with NIST SP 800-171 or by another DFARS contract provision. Encryption used for other purposes, such as within applications or devices within the protected environment of the covered contractor information system, would not need to be FIPS-validated. Note that any separate contract requirement (not currently in NIST SP 800-171) to encrypt data at rest (e.g., PII) within the information system would require use of FIPS validated cryptography.

Encryption, though preferred, is not required if using common-carrier provided Multiprotocol Label Switching (MPLS) private network, as the MPLS separation provides sufficient protection without encryption.

Transport Layer Security (TLS) protocol can be used to protect CUI during transmission over the internet. The current version of TLS (TLS 1.2) is preferred. If earlier versions must be used to interact with certain organizations, the servers shall not support Secure Sockets Layer (SSL) version 3.0 or earlier. The cryptographic module used by the server and client must be a FIPS 140-validated cryptographic module. All cryptographic algorithms that are included in the configured cipher suites must be within the scope of the validation, as well as the random number generator. For further information see NIST SP 800-52, rev 1, "Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations."
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r1. pdf

Where to Look:

- system and communications protection policy
- procedures addressing transmission confidentiality and integrity
- information system design documentation
- information system configuration settings and associated documentation
- information system audit records
- other relevant documents or records

Who to Talk to:

- system/network administrators
- employees with information security

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

responsibilities

- system developers

Perform Test On:

- automated mechanisms supporting and/or implementing transmission confidentiality and/ or integrity
- cryptographic mechanisms supporting and/or implementing transmission confidentiality and/ or integrity
- automated mechanisms supporting and/or implementing alternative physical safeguards
- processes for defining and implementing alternative physical safeguards

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.13.9 *Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.*

Does the system terminate a network connection at the end of a session or after a defined timeframe of inactivity?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

This requirement applies to both internal and external networks. Time periods of inactivity may be established by companies and include time periods by type of network access or for specific network accesses.

Terminating network connections associated with communications sessions include, for example, de-allocating associated TCP/IP address/port pairs at the operating system level, or de-allocating networking assignments at the application level if multiple application sessions are using a single, operating system-level network connection.

Where to Look:

- system and communications protection policy
- procedures addressing network disconnect
- information system design documentation
- security plan
- information system
- configuration settings and associated documentation
- information system audit records
- other relevant documents or records

Who to Talk to:

- system/network administrators
- employees with information security responsibilities
- system developers

Perform Test On:

- automated mechanisms supporting and/or implementing network disconnect capability

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.13.10 Establish and manage cryptographic keys for cryptography employed in the organization systems.

Are processes and automated mechanisms used to provide key management within the information system?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

Cryptographic key management system provide for the management of cryptographic keys and their metadata including generation, distribution, storage, backup, archive, recovery, use, revocation, and destruction.

Where to Look:

- system and communications protection policy
- procedures addressing cryptographic key establishment and management
- information system design documentation
- cryptographic mechanisms
- information system configuration settings and associated documentation
- information system audit records
- other relevant documents or records

Who to Talk to:

- system/network administrators
- employees with information security responsibilities
- employees with responsibilities for cryptographic key establishment and/or management

Perform Test On:

- automated mechanisms supporting and/or implementing cryptographic key establishment and management

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.13.11 Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.

Is FIPS-validated cryptography used to protect CUI?

Yes No Partially Does Not Apply Alternative Approach

Do communication cryptographic mechanisms comply with applicable policies, standards, and guidance?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

Cryptography can be employed to support a variety of security solutions including the protection of CUI, the provision of digital signatures, and the enforcement of information separation when authorized individuals have the necessary clearances for such information but lack the necessary formal access approvals. Cryptography can also be used to support random number generation and hash generation. Generally applicable cryptographic standards include FIPS-validated cryptography.

The NIST SP 800-171 requirements for cryptography used to protect the confidentiality of CUI must use FIPS-validated cryptography, which means the cryptographic module must have been tested and validated to meet FIPS 140-1 or -2 requirements. Simply using an approved algorithm (e.g., FIPS 197 for AES) is not sufficient. The module (software and/ or hardware) used to implement the algorithm must be separately validated under FIPS 140. When an application or device allows a choice (by selecting FIPS-mode or not), then the FIPS-mode has been validated under FIPS 140-2, but the other options (non- FIPS) allow certain operations that would not meet the FIPS requirements. More information is available at

http://csrc.nist.gov/groups/STM/cmvp/

When NIST SP 800-171 requires cryptography, it is to protect the confidentiality of CUI. Accordingly, FIPS-validated cryptography is required to protect CUI, typically when transmitted or stored outside the protected environment of the covered contractor information system (including wireless/remote access) if not separately protected (e.g., by a protected distribution system). FIPS-validated cryptography is required whenever the encryption is required to protect covered defense information in accordance with NIST SP 800-171 or by another DFARS contract provision. Encryption used for other purposes, such as within applications or devices within the protected environment of the covered contractor information system, would not need to be FIPS-validated. Note that any separate contract requirement (not currently in NIST SP 800-171) to encrypt data at rest (e.g., PII) within the information system would require use of FIPS-validated cryptography.

Where to Look:

- system and communications protection policy
- procedures addressing cryptographic protection
- information system design documentation
- information system configuration settings and associated documentation
- cryptographic module validation certificates
- list of FIPS validated cryptographic modules
- information system audit records
- other relevant documents or records

Who to Talk to:

- system/network administrators
- employees with information security responsibilities
- system developers
- employees with responsibilities for cryptographic protection

Perform Test On:

- automated mechanisms supporting and/or implementing cryptographic protection

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.13.12 Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.

Have collaborative computing devices (e.g., cameras, microphones, etc.) been configured so they cannot be remotely activated?

Yes No Partially Does Not Apply Alternative Approach

Are users notified when collaborative computing devices are in use?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

Collaborative computing devices include, for example, networked white boards, cameras, and microphones. Indication of use includes signals to users when collaborative computing devices are activated.

Where to Look:

- system and communications protection policy
- procedures addressing collaborative computing
- access control policy and procedures
- information system design documentation
- information system configuration settings and associated documentation
- information system audit records
- other relevant documents or records

Who to Talk to:

- system/network administrators
- employees with information security responsibilities
- system developers
- employees with responsibilities for managing collaborative computing devices

Perform Test On:

- automated mechanisms supporting and/or implementing management of remote activation of collaborative computing devices
- automated mechanisms providing an indication of use of collaborative computing devices

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.13.13 Control and monitor the use of mobile code.

Are there defined limits of mobile code usage, established usage restrictions, that specifically authorize use of mobile code (e.g., Java, JavaScript, ActiveX, PDF, Flash, Shockwave, Postscript, VBScript, etc.) within the information system?

Yes No Partially Does Not Apply Alternative Approach

Is the use of mobile code documented, monitored, and managed? (Java, JavaScript, ActiveX, PDF, Flash, Shockwave, Postscript, VBScript, etc.)

Yes No Partially Does Not Apply Alternative Approach

Additional Information

Decisions regarding the employment of mobile code within company information systems are based on the potential for the code to cause damage to the systems if used maliciously. Mobile code technologies include, for example, Java, JavaScript, ActiveX, Postscript, PDF, Shockwave movies, Flash animations, and VBScript. Usage restrictions and implementation guidance apply to both the selection and use of mobile code installed on servers and mobile code downloaded and executed on individual workstations and devices (e.g., smart phones). Mobile code policy and procedures address preventing the development, acquisition, or introduction of unacceptable mobile code within company information systems.

This requirement is necessary to protect the overall system processing CUI; it is not about software used to actually process CUI.

Where to Look:

- system and communications protection policy
- procedures addressing mobile code
- mobile code usage restrictions
- mobile code implementation policy and procedures
- list of acceptable mobile code and mobile code technologies
- list of unacceptable mobile code and mobile technologies
- authorization records
- information system monitoring records
- information system audit records
- other relevant documents or records

Who to Talk to:

- system/network administrators
- employees with information security responsibilities
- employees with responsibilities for managing mobile code

Perform Test On:

- process for controlling, authorizing, monitoring, and restricting mobile code
- automated mechanisms supporting and/or implementing the management of mobile code
- automated mechanisms supporting and/or implementing the monitoring of mobile code

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.13.14 Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.

Is the use of VoIP controlled?

Yes No Partially Does Not Apply Alternative Approach

Is the use of VoIP authorized, and monitored?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

Voice Over Internet Protocol (VoIP) is a type of hardware and software that enables people to use the internet as the transmission pathway for telephone calls. VoIP sends voice data in packets by means of internet protocols (IP) instead of using traditional circuit transmissions of the public switched telephone network (PSTN).

Both the voice and data worlds come with the inherent IP security risks, when using the traditional voice side of the network through the application of VoIP. VoIP use necessitates security measures such as encrypting voice services, building redundancy into VoIP networks, locking down VoIP servers, and performing regular security audits on the network. It is also important that VoIP equipment is properly secured, it should be placed behind firewalls, and patched against vulnerabilities. VoIP should be monitored frequently using intrusion-detection systems.

If VoIP is physically or cryptographically isolated from the information systems processing CUI, this security requirement would not apply. However it is still prudent to control who uses VoIP since CUI could be taken from the information system and communicated via a VoIP system. Policies and procedures are needed to ensure CUI remains within the system that stores and processes it. See 3.1.2, 3.1.3, and 3.1.4 in the Access Control Family.

Where to Look:

- system and communications protection policy
- procedures addressing VoIP
- VoIP usage restrictions
- VoIP implementation guidance
- information system design documentation
- information system configuration settings and associated documentation
- information system monitoring records
- information system audit records
- other relevant documents or records

Who to Talk to:

- system/network administrators
- employees with information security responsibilities
- employees with responsibilities for managing VoIP

Perform Test On:

- process for authorizing, monitoring, and controlling VoIP
- automated mechanisms supporting and/or implementing authorizing, monitoring, and controlling VoIP

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.13.15 Protect the authenticity of communications sessions.

Are implemented controls in place to protect session communications (e.g., the controls implemented to validate identities and information transmitted to protect against man-in-the-middle attacks, session hijacking, and insertion of false information into sessions)?

Yes No Partially Does Not Apply Alternative Approach

Does the system provide mechanisms to protect the authenticity of device-to-device communications sessions?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

This requirement addresses communications protection at the session, versus packet level (e.g., sessions in service-oriented architectures providing web-based services), and establishes grounds for confidence at both ends of communications sessions in ongoing identities of other parties and in the validity of information transmitted. Authenticity protection includes protecting against man-in-the-middle attacks/session hijacking and the insertion of false information into sessions.

Where to Look:

- system and communications protection policy
- procedures addressing session authenticity
- information system design documentation
- information system configuration settings and associated documentation
- information system audit records
- other relevant documents or records

Who to Talk to:

- system/network administrators
- employees with information security responsibilities

Perform Test On:

- automated mechanisms supporting and/or implementing session authenticity

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.13.16 Protect the confidentiality of CUI at rest.

Are there controls used to protect CUI while stored in company information systems?

Yes No Partially Does Not Apply Alternative Approach

Does the system protect the confidentiality of information at rest?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

This requirement addresses the confidentiality of information at rest and covers user information and system information. Information at rest refers to the state of information when it is located on storage devices as specific components of information systems. System-related information requiring protection includes configurations or rule sets for firewalls, gateways, intrusion detection/prevention systems, filtering routers, and authenticator content. Companies may also employ other security requirements including secure off-line storage in lieu of online storage when adequate protection of information at rest cannot otherwise be achieved and/or continuous monitoring to identify malicious code at rest.

CUI can be stored at rest in any non-mobile devices or data center, unencrypted, as long as it is protected by other approved logical or physical methods. The mapped NIST SP 800-53, "Security Controls and Assessment Procedures for Federal Information Systems and Organizations," control (SC-8), notes that this requirement is to protect the confidentiality of CUI information at rest when it is located on storage devices as specific components of information systems and that "organizations may employ different mechanisms to achieve confidentiality protection, including the use of cryptographic mechanisms and file share scanning." Thus, encryption is an option, not a requirement.

Where to Look:

- system and communications protection policy
- procedures addressing protection of information at rest
- information system design documentation
- information system configuration settings and associated documentation
- cryptographic mechanisms and associated configuration documentation
- list of information at rest requiring confidentiality and integrity protections
- other relevant documents or records

Who to Talk to:

- system/network administrators
- employees with information security responsibilities
- system developers

Perform Test On:

- automated mechanisms supporting and/or implementing confidentiality and integrity protections for information at rest

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

System and Information Integrity: SP 800-171 Security Family 3.14

Integrity is defined as guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. It is the assertion that data can only be accessed or modified by the authorized employees. System and information integrity provides assurance that the information being accessed has not been meddled with or damaged by an error in the system. Examples of system and information integrity requirements include: flaw remediation, malicious code protection, security function verification, information input validation, error handling, non-persistence, and memory protection.

Companies should

- identify, report, and correct information and system flaws in a timely manner,
- provide protection from malicious code at appropriate locations within company systems, and
- monitor system security alerts and advisories and respond appropriately.

The following security requirements fall under the System and Information Integrity family:

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.14.1 *Identify, report, and correct information and information system flaws in a timely manner.*

Are system flaws identified, reported, and corrected within company-defined time periods?

Yes No Partially Does Not Apply Alternative Approach

Does the company perform all security-relevant software updates (patching, service packs, hot fixes, and anti-virus signature additions) in response to identified system flaws and vulnerabilities within the timeframe specified in policy or within the system security plan?

Yes No Partially Does Not Apply Alternative Approach

When available, do managers and administrators of the system rely on centralized management of the flaw remediation process, to include the use of automated update software, patch management tools, and automated status scanning?

Yes No Partially Does Not Apply Alternative Approach

Is the time between flaw identification and flaw remediation measured and compared with benchmarks?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

Companies identify information systems affected by announced software flaws including potential vulnerabilities resulting from those flaws, and report this information to employees with information security responsibilities. Security-relevant software updates include patches, service packs, hot fixes, and anti- virus signatures. Organizations also address flaws discovered during security assessments, continuous monitoring, incident response activities, and system error handling. Organizations take advantage of available resources such as the Common Weakness Enumeration (CWE) or Common Vulnerabilities and Exposures (CVE) databases in remediating flaws discovered in company information systems.

By incorporating flaw remediation into ongoing configuration management processes, required/ anticipated remediation actions can be tracked and verified. Flaw remediation actions that can be tracked and verified include, for example, determining whether organizations follow US-CERT guidance and Information Assurance Vulnerability Alerts. Organization-defined time periods for updating security-relevant software and firmware may vary based on a variety of factors including, for example, the security category of the information system or the criticality of the update (i.e., severity of the vulnerability related to the discovered flaw). Some types of flaw remediation may require more testing than other types. Companies determine the degree and type of testing needed for the specific type of flaw remediation activity under consideration and the types of changes that are to be configuration-managed. In some situations, companies may determine that the testing of software and/or firmware updates is not necessary or practical, for example, when implementing simple anti-virus signature updates. Companies may also consider in testing decisions, whether security-relevant software or firmware updates are obtained from authorized sources with appropriate digital signatures.

Where to Look:

- system and information integrity policy
- configuration management policy and procedures
- procedures addressing flaw remediation
- procedures addressing configuration management
- procedures addressing malicious code
- procedures addressing security alerts, advisories, and directives
- records of security alerts and advisories
- malicious code protection mechanisms
- records of malicious code protection update
- information system design documentation
- information system configuration settings and associated documentation
- scan results from malicious code protection mechanisms
- record of actions initiated by malicious code protection mechanisms in response to malicious code detection
- information system audit records
- list of flaws and vulnerabilities potentially affecting the information system
- list of recent security flaw remediation actions performed on the information system (e.g., list of installed patches, service packs, hot fixes, and other software updates to correct information system flaws)

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

- test results from the installation of software and firmware updates to correct information system flaws
- installation/change control records for security-relevant software and firmware updates
- other relevant documents or records

Who to Talk to:

- employees installing, configuring, and/or maintaining the information system
- employees with responsibility for flaw remediation
- employees with configuration management responsibility
- employees with responsibility for malicious code protection
- employees with security alert and advisory responsibilities
- employees implementing, operating, maintaining, and using the information system
- employees, company elements, and/or external organizations to whom alerts, advisories, and directives are to be disseminated
- system/network administrators
- employees with information security responsibilities

Perform Test On:

- processes for identifying, reporting, and correcting information system flaws
- process for installing software and firmware updates
- automated mechanisms supporting and/ or implementing reporting, and correcting information system flaws
- automated mechanisms supporting and/or implementing testing software and firmware updates
- processes for employing, updating, and configuring malicious code protection mechanisms
- process for addressing false positives and resulting potential impact
- automated mechanisms supporting and/ or implementing employing, updating, and configuring malicious code protection mechanisms
- automated mechanisms supporting and/or implementing malicious code scanning and subsequent actions
- processes for defining, receiving, generating, disseminating, and complying with security alerts, advisories, and directives
- automated mechanisms supporting and/or implementing definition, receipt, generation, and dissemination of security alerts, advisories, and directives
- automated mechanisms supporting and/or implementing security directives

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.14.2 *Provide protection from malicious code at appropriate locations within organization information systems.*

Does the company employ malicious code protection mechanisms at system entry and exit points to minimize the presence of malicious code? System entry and exit points may include firewalls, electronic mail servers, web servers, proxy servers, remote- access servers, workstations, notebook computers, and mobile devices.

Yes No Partially Does Not Apply Alternative Approach

Does the system automatically update malicious code protection mechanisms?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

Malicious code protection mechanisms (e.g., anti-virus, anti-malware and anti-spyware) include, for example, signature definitions, heuristics, and behavior analyzers. Due to information system integrity and availability concerns, companies should consider the methodology used to carry out automatic updates.

Where to Look:

- system and information integrity policy
- configuration management policy and procedures
- procedures addressing flaw remediation
- procedures addressing configuration management
- procedures addressing malicious code protection
- procedures addressing security alerts, advisories, and directives
- records of security alerts and advisories other relevant documents or records
- malicious code protection mechanisms
- records of malicious code protection update
- information system design documentation
- information system configuration settings and associated documentation
- scan results from malicious code protection mechanisms
- record of actions initiated by malicious code protection mechanisms in response to malicious code detection
- information system audit records
- list of flaws and vulnerabilities potentially affecting the information system
- list of recent security flaw remediation actions performed on the information system (e.g., list of installed patches, service packs, hot fixes, and other software updates to correct information system flaws)
- test results from the installation of software and firmware updates to correct information system flaws installation/change control records for security-relevant software and firmware updates
- other relevant documents or records

Who to Talk to:

- system/network administrators
- employees with information security responsibilities
- employees installing, configuring, and/or maintaining the information system
- employees with responsibility for flaw remediation
- employees with responsibility for malicious code protection
- employees with security alert and advisory responsibilities
- employees implementing, operating, maintaining, and using the information system
- employees, and/or external organizations to whom alerts, advisories, and directives are to be disseminated
- employees with configuration management responsibility

Perform Test On:

- processes for identifying, reporting, and correcting information system flaws
- process for installing software and firmware updates

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

- automated mechanisms supporting and/ or implementing reporting, and correcting information system flaws
- automated mechanisms supporting and/or implementing testing software and firmware updates
- processes for employing, updating, and configuring malicious code protection mechanisms process for addressing false positives and resulting potential impact
- automated mechanisms supporting and/ or implementing employing, updating, and configuring malicious code protection mechanisms
- automated mechanisms supporting and/or implementing malicious code scanning and subsequent actions
- processes for defining, receiving, generating, disseminating, and complying with security alerts, advisories, and directives
- automated mechanisms supporting and/or implementing definition, receipt, generation, and dissemination of security alerts, advisories, and directives
- automated mechanisms supporting and/or implementing security directives

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.14.3 *Monitor information system security alerts and advisories and take appropriate actions in response.*

Does the company receive security alerts, advisories, and directives from reputable external organizations?

Yes No Partially Does Not Apply Alternative Approach

Does the company disseminate this information to individuals with need-to-know in the company?

Yes No Partially Does Not Apply Alternative Approach

Are alerts responded to in a timely manner?

Yes No Partially Does Not Apply Alternative Approach

Are internal security alerts, advisories, and directives generated?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

The United States Computer Emergency Readiness Team (US-CERT) generates security alerts and advisories to maintain situational awareness: https://www.us-cert.gov/

Security directives are issued by designated organizations with the responsibility and authority to issue such directives. Compliance with security directives is essential due to the critical nature of many of these directives and the potential immediate adverse effects on company operations and assets, individuals, and other organizations, should the directives not be implemented in a timely manner. External organizations include, for example, external mission/business partners, supply chain partners, external service providers, and other peer/supporting organizations.

Cleared defense contractors are eligible for the Defense Industrial Base (DIB) Cybersecurity program, which is a voluntary cyber threat information sharing program between DOD and DIB participants. Under this partnership, the DOD Cyber Crime Center receives voluntary reporting from DIB participants and makes available to all the other DIB participants, as well as indicators from Government sources. See https://dibnet.dod.mil/portal/intranet/

Where to Look:

- system and information integrity policy
- configuration management policy and procedures
- procedures addressing flaw remediation
- procedures addressing malicious code protection
- procedures addressing security alerts, advisories, and directives records of security alerts and advisories
- malicious code protection mechanisms
- records of malicious code protection update
- information system design documentation
- information system configuration settings and associated documentation
- scan results from malicious code protection mechanisms
- record of actions initiated by malicious code protection mechanisms in response to malicious code detection
- information system audit records
- list of flaws and vulnerabilities potentially affecting the information system
- list of recent security flaw remediation actions performed on the information system (e.g., list of installed patches, service packs, hot fixes, and other software updates to correct information system flaws)
- testing results from the installation of software and firmware updates to correct information system flaws
- installation/change control records for security-relevant software and firmware updates
- other relevant documents or records

Who to Talk to:

- employees installing, configuring, and/or maintaining the information system
- employees with responsibility for flaw remediation
- employees with responsibility for malicious code protection
- employees with configuration management responsibility
- employees with security alert and advisory responsibilities
- employees implementing, operating, maintaining, and using the information system
- employees, company elements, and/or external

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

organizations to whom alerts, advisories, and directives are to be disseminated

- system/network administrators
- employees with information security responsibilities

Perform Test On:

- processes for identifying, reporting, and correcting information system flaws
- process for installing software and firmware updates
- automated mechanisms supporting and/ or implementing reporting, and correcting information system flaws
- automated mechanisms supporting and/or implementing test software and firmware updates
- processes for employing, updating, and configuring malicious code protection mechanisms process for addressing false positives and resulting potential impact
- automated mechanisms supporting and/ or implementing employing, updating, and configuring malicious code protection mechanisms
- automated mechanisms supporting and/or implementing malicious code scanning and subsequent actions
- processes for defining, receiving, generating, disseminating, and complying with security alerts, advisories, and directives
- automated mechanisms supporting and/or implementing definition, receipt, generation, and dissemination of security alerts, advisories, and directives
- automated mechanisms supporting and/or implementing security directives

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.14.4 *Update malicious code protection mechanisms when new releases are available.*

Does the company update information system protection mechanisms (e.g., anti-virus signatures) within 5 days of new releases?

Yes No Partially Does Not Apply Alternative Approach

Are these updates completed in accordance with configuration management policy and procedures?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

Malicious code includes viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats (e.g., UUENCODE, Unicode), contained within compressed or hidden files, or hidden in files using steganography. Malicious code can be transported by different means including web accesses, electronic mail, electronic mailattachments, and portable storage devices. Malicious code insertions occur through the exploitation of information system vulnerabilities. Malicious code protection mechanisms include anti-virus signature definitions and reputation- based technologies. A variety of technologies and methods exist to limit or eliminate the effects of malicious code. Pervasive configuration management and comprehensive software integrity controls may be effective in preventing execution of unauthorized code. In addition to commercial off-the-shelf software, malicious code may also be present in custom-built software. This could include logic bombs, back doors, and other types of cyber-attacks that could affect company business functions. Traditional malicious code protection mechanisms cannot always detect such code. In these situations, companies should rely instead on other safeguards including secure coding practices, configuration management and control, trusted procurement processes, and monitoring practices to help ensure that software does not perform functions other than those intended. Companies may determine that in response to the detection of malicious code, different actions may be warranted. For example, companies can define actions in response to malicious code detection during periodic scans, actions in response to detection of malicious downloads, and/ or actions in response to detection of maliciousness when attempting to open or execute files.

Where to Look:

- system and information integrity policy
- configuration management policy and procedures
- procedures addressing flaw remediation
- procedures addressing configuration management
- procedures addressing malicious code protection
- procedures addressing security alerts, advisories, and directives
- records of security alerts and advisories other relevant documents or records
- malicious code protection mechanisms
- records of malicious code protection update
- information system design documentation
- information system configuration settings and associated documentation
- scan results from malicious code protection mechanisms
- record of actions initiated by malicious code protection mechanisms in response to malicious code detection
- information system audit records
- list of flaws and vulnerabilities potentially affecting the information system
- list of recent security flaw remediation actions performed on the information system (e.g., list of installed patches, service packs, hot fixes, and other software updates to correct information system flaws)
- test results from the installation of software and firmware updates to correct information system flaws installation/change control records for security-relevant software and firmware updates
- other relevant documents or records

Who to Talk to:

- system/network administrators
- employees with information security responsibilities
- employees installing, configuring, and/or maintaining the information system

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

- employees with responsibility for flaw remediation
- employees with responsibility for malicious code protection
- employees with security alert and advisory responsibilities
- employees implementing, operating, maintaining, and using the information system
- employees, and/or external organizations to whom alerts, advisories, and directives are to be disseminated
- employees with configuration management responsibility

Perform Test On:

- processes for identifying, reporting, and correcting information system flaws
- process for installing software and firmware updates
- automated mechanisms supporting and/ or implementing reporting, and correcting information system flaws
- automated mechanisms supporting and/or implementing testing software and firmware updates
- processes for employing, updating, and configuring malicious code protection mechanisms process for addressing false positives and resulting potential impact
- automated mechanisms supporting and/ or implementing employing, updating, and configuring malicious code protection mechanisms
- automated mechanisms supporting and/or implementing malicious code scanning and subsequent actions
- processes for defining, receiving, generating, disseminating, and complying with security alerts, advisories, and directives
- automated mechanisms supporting and/or implementing definition, receipt, generation, and dissemination of security alerts, advisories, and directives
- automated mechanisms supporting and/or implementing security directives

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.14.5 *Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.*

Does the company perform periodic scans of the information system for malware? Are scans performed within the timeframe specified in policy or within the system security plan?

Yes No Partially Does Not Apply Alternative Approach

Does the company perform real-time scans of files from external sources as the files are downloaded, opened, or executed?

Yes No Partially Does Not Apply Alternative Approach

Does the system disinfect and quarantine infected files?

Yes No Partially Does Not Apply Alternative Approach

Where to Look:

- system and information integrity policy
- configuration management policy and procedures
- procedures addressing malicious code protection
- malicious code protection mechanisms
- records of malicious code protection update
- information system design documentation
- information system configuration settings and associated documentation
- scan results from malicious code protection mechanisms
- record of actions initiated by malicious code protection mechanisms in response to malicious code detection
- information system audit records
- other relevant documents or records

Who to Talk to:

- system/network administrators
- employees with information security responsibilities
- employees installing, configuring, and/or maintaining the information system
- employees with responsibility for malicious code protection
- employees with configuration management responsibility

Perform Test On:

- processes for employing, updating, and configuring malicious code protection mechanisms process for addressing false positives and resulting potential impact
- automated mechanisms supporting and/ or implementing employing, updating, and configuring malicious code protection mechanisms
- automated mechanisms supporting and/or implementing malicious code scanning and subsequent actions

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.14.6 *Monitor the information system including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.*

Does the company monitor the information system to detect attacks and indicators of potential attacks, as well as unauthorized local, network, and remote connections?

Yes No Partially Does Not Apply Alternative Approach

Will the company strategically deploy monitoring devices within the information system to collect essential information?

Yes No Partially Does Not Apply Alternative Approach

Is the information gained from these monitoring tools protected from unauthorized access, modification, and deletion?

Yes No Partially Does Not Apply Alternative Approach

Does the system monitor inbound and outbound communications for unusual or unauthorized activities or conditions?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

Unusual/unauthorized activities or conditions related to information system inbound and outbound communications traffic include internal traffic that indicates the presence of malicious code within company information systems or propagating among system components, the unauthorized exporting of information, or signaling to external information systems.

Evidence of malicious code is used to identify potentially compromised information systems or information system components. Monitoring of these communications may indicate or detect potential attacks to the company's information system.

Where to Look:

- continuous monitoring strategy
- system and information integrity policy
- procedures addressing information system monitoring tools and techniques
- facility diagram/layout information
- system design documentation
- information system monitoring tools and techniques
- documentation locations within information system where monitoring devices are deployed
- information system configuration settings and associated documentation
- information system protocols
- information system audit records
- other relevant documents or records

Who to Talk to:

- system/network administrators
- employees with information security responsibilities
- employees installing, configuring, and/or maintaining the information system
- employees with responsibility monitoring the information system
- employees with responsibility for the intrusion detection system

Perform Test On:

- processes for information system monitoring
- automated mechanisms supporting and/or implementing information system monitoring capability
- processes for intrusion detection/information system monitoring
- automated mechanisms supporting and/or implementing intrusion detection capability/ information system monitoring
- automated mechanisms supporting and/or implementing monitoring of inbound/ outbound communications traffic

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

3.14.7 *Identify unauthorized use of the information system.*

Does the company monitor the information system to identify unauthorized access and use?

Yes No Partially Does Not Apply Alternative Approach

Does the company monitor the information for potential misuse?

Yes No Partially Does Not Apply Alternative Approach

Is unauthorized use of the system identified (e.g., log monitoring)?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

Information system monitoring includes external and internal monitoring. External monitoring includes the observation of events occurring at the information system boundary (i.e., part of perimeter defense and boundary protection). Internal monitoring includes the observation of events occurring within the information system.

Companies can monitor information systems by observing audit activities in real time or by observing other system aspects such as access patterns, characteristics of access, and other actions. The monitoring objectives may guide determination of the events. Information system monitoring capability is achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, scanning tools, audit record monitoring software, network monitoring software). Strategic locations for monitoring devices include selected perimeter locations and near server farms supporting critical applications, with such devices typically being employed at the managed interfaces.

The granularity of monitoring information collected is based on company monitoring objectives and the capability of information systems to support such objectives. Specific types of transactions of interest include, for example, hyper text transfer protocol (HTTP) traffic that bypasses HTTP proxies.

Information system monitoring is an integral part of company continuous monitoring and incident response programs. Output from system monitoring serves as input to continuous monitoring and incident response programs. A network connection is any connection with a device that communicates through a network (e.g., local area network, internet). A remote connection is any connection with a device communicating through an external network (e.g., the internet). Local, network, and remote connections can be either wired or wireless.

Where to Look:

- continuous monitoring strategy
- system and information integrity policy
- procedures addressing information system monitoring tools and techniques
- facility diagram/layout information
- system design documentation
- information system monitoring tools and techniques
- documentation locations within information system where monitoring devices are deployed
- information system configuration settings and associated documentation
- other relevant documents or records

Who to Talk to:

- system/network administrators
- employees with information security responsibilities
- employees installing, configuring, and/or maintaining the information system
- employees with responsibility monitoring the information system

Perform Test On:

- processes for information system monitoring
- automated mechanisms supporting and/or implementing information system monitoring capability

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

Glossary

Access Control - The process of granting or denying specific requests to: 1) obtain and use information and related information processing services and 2) enter specific physical facilities (e.g., federal buildings, military establishments, border crossing entrances).

Accountability - The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports nonrepudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action.

Adware - Advertising-supported software is any software package that automatically renders advertisements to generate revenue for its author. The advertisements may be in the user interface of the software or on a screen presented to the user during the installation process. The functions may be designed to analyze which internet sites the user visits and to present advertising pertinent to the types of goods or services featured there. Unwanted advertisements are considered malware.

Assurance - Grounds for confidence that the other four security goals (integrity, availability, confidentiality, and accountability) have been adequately met by a specific implementation. "Adequately met" includes 1) functionality that performs correctly, 2) sufficient protection against unintentional errors (by users or software), and 3) sufficient resistance to intentional penetration or by-pass.

Attack - Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself.

Audit - Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures.

Audit log - Chronological record of system activities, including records of system accesses and operations performed in a given period.

Audit record - Individual entry in an audit log related to an audited event.

Authentication - Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in a system.

Authorization - The official management decision given by a senior official to authorize operation of a system or the common controls inherited by designated organizations systems and to explicitly accept the risk to company operations (including mission, functions, image, and reputation), company assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security and privacy controls. Also known as authorization to operate (ATO).

Authorizing Official (AO) - A senior (federal) official or executive with the authority to formally assume responsibility for operating a system at an acceptable level of risk to company operations (including mission, functions, image, or reputation), company assets, individuals, other organizations, and the Nation.

Availability - Ensuring timely and reliable access to and use of information.

Back Door - An undocumented way of gaining access to computer system. A backdoor is a potential security risk.

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

Baseline Configuration - A documented set of specifications for a system, or a configuration item within a system, that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures.

Blacklisting - A process used to identify software programs that are not authorized to execute on a system or prohibited Universal Resource Locators (URL)/websites.

Biometrics - A measurable physical characteristic or personal behavioral trait used to recognize the identity, or verify the claimed identity, of an applicant. Facial images, fingerprints, and iris scan samples are all examples of biometrics.

Bit - A binary digit having a value of 0 or 1.

Challenge Response Protocol - An authentication protocol where the verifier sends the claimant a challenge (usually a random value or a nonce) that the claimant combines with a secret (often by hashing the challenge and a shared secret together, or by applying a private key operation to the challenge) to generate a response that is sent to the verifier. The verifier can independently verify the response generated by the claimant (such as by re-computing the hash of the challenge and the shared secret and comparing to the response, or performing a public key operation on the response) and establish that the claimant possesses and controls the secret.

Checksum - A value that 1) is computed by a function that is dependent on the content of a data object and 2) is stored or transmitted together with the object, for detecting changes in the data.

Ciphertext - Data in its encrypted form.

Confidentiality - Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

Configuration Management - A collection of activities focused on establishing and maintaining the integrity of information technology products and systems, through control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development life cycle.

Configuration Settings - The set of parameters that can be changed in hardware, software, or firmware that affect the security posture and/or functionality of the system.

Controlled Area - Any area or space for which the organization has confidence that the physical and procedural protections provided are sufficient to meet the requirements established for protecting the information or system.

Controlled Unclassified Information (CUI) - Information that law, regulation, or government wide policy requires to have safeguarding or disseminating controls, excluding information that is classified under Executive Order 13526, Classified National Security Information, December 29, 2009, or any predecessor or successor order, or the Atomic Energy Act of 1954, as amended.

CUI Categories or Subcategories - Those types of information for which laws, regulations, or government wide policies require or permit agencies to exercise safeguarding or dissemination controls, and which the CUI Executive Agent has approved and listed in the CUI Registry.

CUI Executive Agent - The National Archives and Records Administration (NARA), which implements the executive branch-wide CUI Program and oversees federal agency actions to

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

comply with Executive Order 13556 “Controlled Unclassified Information”. NARA has delegated this authority to the Director of the Information Security Oversight Office (ISOO).

CUI Program - The executive branch-wide program to standardize CUI handling by all federal agencies. The program includes the rules, organization, and procedures for CUI, established by Executive Order 13556, 32 CFR Part 2002, and the CUI Registry.

CUI Registry - The online repository for all information, guidance, policy, and requirements on handling CUI, including everything issued by the CUI Executive Agent other than 32 CFR Part 2002. Among other information, the CUI Registry identifies all approved CUI categories and subcategories, provides general descriptions for each, identifies the basis for controls, establishes markings, and includes guidance on handling procedures.

Countermeasures - Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system.

Denial of Service - The prevention of authorized access to resources or the delaying of time-critical operations. (Time-critical may be milliseconds or it may be hours, depending upon the service provided.)

Decoding - The conversion of an encoded format back into the original sequence of characters.

Digital Signature - The result of a cryptographic transformation of data which, when properly implemented, provides the services of: 1) origin authentication, 2) data integrity, and 3) signer non-repudiation.

Encoding - To convert into a coded form; the process of putting a sequence of characters (letters, numbers, punctuation, and certain symbols) into a specialized format for efficient transmission or storage.

Encryption - The cryptographic transformation of data to produce ciphertext.

End-to-End Encryption - Communications encryption in which data is encrypted when being passed through a network, but routing information remains visible.

Environment of Operation - The physical surroundings in which a system processes, stores, and transmits information.

Executive Agency - An executive department specified in 5 U.S.C., Sec. 105; a military department specified in 5 U.S.C., Sec. 102; an independent establishment as defined in 5 U.S.C., Sec. 104(1); and a wholly owned Government corporation fully subject to the provisions of 31 U.S.C., Chapter 91.

External System (or component) - A system or component of a system that is outside of the authorization boundary established by the organization and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness.

External System Service - A system service that is implemented outside of the authorization boundary of the organizational system (i.e., a service that is used by, but not a part of, the organizational system) and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness.

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

External System Service Provider - A provider of external system services to an organization through a variety of consumer-producer relationships including but not limited to: joint ventures; business partnerships; outsourcing arrangements (i.e., through contracts, interagency agreements, lines of business arrangements); licensing agreements; and/or supply chain exchanges.

External Network - A network not controlled by the organization.

Federal Information System - An information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.

FIPS-validated cryptography - A cryptographic module validated by the Cryptographic Module Validation Program (CMVP) to meet requirements specified in FIPS Publication 140-2 (as amended). As a prerequisite to CMVP validation, the cryptographic module is required to employ a cryptographic algorithm implementation that has successfully passed validation testing by the Cryptographic Algorithm Validation Program (CAVP).

Firewall - A gateway that limits access between networks in accordance with local security policy.

Firmware - Computer programs and data stored in hardware, typically in read-only memory (ROM) or programmable read-only memory (PROM), such that the programs and data cannot be dynamically written or modified during execution of the programs.

Gateway - An intermediate system (interface, relay) that attaches to two (or more) computer networks that have similar functions but dissimilar implementations and that enables either one-way or two-way communication between the networks.

Hacker - A person who circumvents security and breaks into a network, computer, file, etc., usually with malicious intent.

Hardware - The physical components of a system.

Identifier - Unique data used to represent a person’s identity and associated attributes. A name or a card number are examples of identifiers. A unique label used by a system to indicate a specific entity, object, or group.

Impact - The effect on organizational operations, organizational assets, individuals, other organizations, or the Nation (including the national security interests of the United States) of a loss of confidentiality, integrity, or availability of information or a system.

Impact Value - The assessed potential impact resulting from a compromise of the confidentiality of information (e.g., CUI) expressed as a value of low, moderate, or high.

Incident - An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of a system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

Industrial Control System (ICS) – A general term that encompasses several types of control systems and associated instrumentation used in industrial production technology, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS),

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

and other smaller control system configurations such as programmable logic controllers (PLC) often found in the industrial sectors and critical infrastructures.

Information -1) Facts and ideas, which can be represented (encoded) as various forms of data. 2) Knowledge, e.g., data, instructions, in any medium or form that can be communicated between system entities.

Information Assurance - Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

Information Flow Control - Procedure to ensure that information transfers within a system are not made in violation of the security policy.

Information Resources - Information and related resources, such as personnel, equipment, funds, and information technology.

Information Security - The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction to provide confidentiality, integrity, and availability.

Information Security Policy - Aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information.

Information Security Risk - The risk to company operations (including mission, functions, image, reputation), company assets, individuals, other organizations, and the Nation due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or a system.

Information System - A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Note: Information systems also include specialized systems such as industrial/process controls systems, telephone switching and private branch exchange (PBX) systems, and environmental control systems.

Information Technology - (A) With respect to an executive agency means any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency, if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency that requires the use - 1) of that equipment or 2) of that equipment to a significant extent in the performance of a service or the furnishing of a product; (B) Includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources; but (C) does not include any equipment acquired by a federal contractor incidental to a federal contract.

Insider Threat - The threat that an insider will use her/his authorized access, wittingly or unwittingly, to do harm to the security of the United States. This threat can include damage to the

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

United States through espionage, terrorism, unauthorized disclosure, or through the loss or degradation of departmental resources or capabilities.

Integrity - Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

Internal Network - A network where establishment, maintenance, and provisioning of security controls are under the direct control of organizational employees or contractors; or the cryptographic encapsulation or similar security technology implemented between organization controlled endpoints, provides the same effect (with regard

to confidentiality and integrity). An internal network is typically organization-owned, yet may be organization- controlled while not being organization-owned.

Intrusion Detection System (IDS) - Software that automates the intrusion detection process.

Key - A parameter used in conjunction with a cryptographic algorithm that determines its operation. Examples applicable to this Standard include: 1) the computation of a digital signature from data, and 2) the verification of a digital signature.

Key Management - The activities involving the handling of cryptographic keys and other related security parameters (e.g., initialization vectors) during the entire lifecycle of the keys, including their generation, storage, establishment, entry and output, use, and destruction.

Keystroke Monitoring - The process used to view or record both the keystrokes entered by a computer user and the computer's response during an interactive session. Keystroke monitoring is usually considered a special case of audit trails.

Least Privilege - The principle that a security architecture should be designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function.

Link Encryption - Encryption of information between nodes of a communications system.

Local Access - Access to an organizational system by a user (or process acting on behalf of a user) communicating through a direct connection without the use of a network.

Logic Bomb - A piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met.

Malicious Code - Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of a system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code.

Malware - See Malicious Code.

Media - Physical devices or writing surfaces including, but not limited to, magnetic tapes, optical disks, magnetic disks, Large-Scale Integration (LSI) memory chips, and printouts (but not including display media) onto which information is recorded, stored, or printed within a system.

Mobile Code - Software programs or parts of programs obtained from remote systems, transmitted across a network, and executed on a local system without explicit installation or execution by the recipient.

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

Mobile Device - A portable computing device that has a small-form factor such that it can easily be carried by a single individual; is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); possesses local, non-removable/removable data storage; and includes a self-contained power source. Mobile devices may also include voice communication capabilities, onboard sensors that allow the devices to capture information, or built-in features that synchronize local data with remote locations. Examples include smartphones, tablets, and E-readers.

Multifactor Authentication - Authentication using two or more different factors to achieve authentication. Factors include something you know (e.g., PIN, password); something you have (e.g., cryptographic identification device, token); or something you are (e.g., biometric).

Network - A system implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.

Network Access - Access to a system by a user (or a process acting on behalf of a user) communicating through a network (e.g., local area network, wide area network, internet).

Node - In data communication, a physical network node may either be a data communication equipment (DCE) such as a modem, hub, bridge or switch; or a data terminal equipment (DTE) such as a digital telephone handset, a printer or a computer, workstation, or a server.

Nonce - A time-varying value that has at most a negligible chance of repeating – for example, a random value that is generated anew for each use, a timestamp, a sequence number, or some combination of these.

Nonfederal Organization - An entity that owns, operates, or maintains a nonfederal information system.

Nonfederal System - A system that does not meet the criteria for a federal system.

Nonlocal Maintenance - Maintenance activities conducted by individuals communicating through a network, either an external network (e.g., the internet) or an internal network.

Password - A string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization.

Penetration Performance Testing - A test methodology in which assessors, typically working under specific constraints, attempt to circumvent or defeat the security features of a system.

Phishing - A technique for attempting to acquire sensitive data, such as bank account numbers, through a fraudulent solicitation in email or on a web site, in which the perpetrator masquerades as a legitimate business or reputable person.

Portable Storage Device - A system component that can be inserted into and removed from a system, and that is used to store data or information (e.g., text, video, audio, and/or image data). Such components are typicallyimplemented on magnetic, optical, or solid state devices (e.g., floppy disks, compact/digital video disks, flash/ thumb drives, external hard disk drives, and flash memory cards/drives that contain nonvolatile memory).

Potential Impact - The loss of confidentiality, integrity, or availability could be expected to have: 1) a limited adverse effect (FIPS Publication 199 low); 2) a serious adverse effect (FIPS

Publication 199 moderate); or 3) a severe or catastrophic adverse effect (FIPS Publication 199 high) on organizational operations, organizational assets, or individuals.

Private Key - A cryptographic key, used with a public key cryptographic algorithm, that is uniquely associated with an entity and is not made public.

Privilege - A right granted to an individual, a program, or a process.

Privileged Account - A system account with authorizations of a privileged user.

Privileged User - A user that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.

Public Key - A cryptographic key used with a public key cryptographic algorithm that is uniquely associated with an entity and that may be made public.

Public Key Cryptography - Encryption system that uses a public-private key pair for encryption and/or digital signature.

Public Key Infrastructure (PKI) - A Framework that is established to issue, maintain, and revoke public key certificates.

Ransomware - Ransomware is a type of malware that blocks access to a device or data until a ransom is paid.

Reciprocity - Mutual agreement among participating enterprises to accept each other's security assessments to reuse information system resources and/or to accept each other's assessed security posture to share information.

Records - The recordings (automated and/or manual) of evidence of activities performed or results achieved (e.g., forms, reports, test results), which serve as a basis for verifying that the organization and the system are performing as intended. Also, used to refer to units of related data fields (i.e., groups of data fields that can be accessed by a program and that contain the complete set of information on particular items).

Remote Access - Access to an organizational system by a user (or a process acting on behalf of a user) communicating through an external network (e.g., the internet).

Remote Maintenance - Maintenance activities conducted by individuals communicating through an external network (e.g., the internet).

Replay Resistance - Protection against the capture of transmitted authentication or access control information and its subsequent retransmission with the intent of producing an unauthorized effect or gaining unauthorized access.

Risk - A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: 1) the adverse impacts that would arise if the circumstance or event occurs and 2) the likelihood of occurrence. Note: System-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or systems and reflect the potential adverse impacts to company operations (including mission, functions, image, or reputation), company assets, individuals, other organizations, and the Nation. Adverse impacts to the Nation include, for example, compromises to systems that support critical

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

infrastructure applications or are paramount to government continuity of operations as defined by the Department of Homeland Security.

Risk Assessment - The process of identifying risks to company operations (including mission, functions, image, and reputation), company assets, individuals, other organizations, and the Nation, resulting from the operation of a system. Part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place. Synonymous with Risk Analysis.

Risk Management - The program and supporting processes to manage information security risk to company operations (including mission, functions, image, reputation), company assets, individuals, other organizations, and the Nation, and includes: 1) establishing the context for risk-related activities, 2) assessing risk, 3) responding to risk once determined, and 4) monitoring risk over time.

Risk Management Framework (RMF) - A structured approach used to oversee and manage risk for an enterprise.

Role - A job function or employment position to which people or other system entities may be assigned in a system.

Safeguards - Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for a system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. Synonymous with security controls and countermeasures.

Sanitization - Actions taken to render data written on media unrecoverable by both ordinary and, for some forms of sanitization, extraordinary means. Process to remove information from media such that data recovery is not possible. It includes removing all classified labels, markings, and activity logs.

Secret Key - A cryptographic key, used with a secret key cryptographic algorithm, that is uniquely associated with one or more entities and should not be made public.

Security - A condition that results from the establishment and maintenance of protective measures that enable an enterprise to perform its mission or critical functions despite risks posed by threats to its use of information systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the enterprise’s risk management approach.

Security Control Assessment - The testing and/or evaluation of the management, operational, and technical security controls in a system 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.

Security Controls - The management, operational, and technical controls, i.e., safeguards or countermeasures) prescribed for a system to protect the confidentiality, integrity, and availability of the system and its information.

Security Engineering - An interdisciplinary approach and means to enable the realization of secure systems. It focuses on defining customer needs, security protection requirements, and

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

required functionality early in the systems development life cycle, documenting requirements, and then proceeding with design, synthesis, and system validation while considering the complete problem.

Security Functionality - The security-related features, functions, mechanisms, services, procedures, and architectures implemented within organizational systems or the environments in which those systems operate.

Security Functions - The hardware, software, or firmware of the system responsible for enforcing the system security policy and supporting the isolation of code and data on which the protection is based.

Security Label - The means used to associate a set of security attributes with a specific information object as part of the data structure for that object.

Security Relevance - Functions or mechanisms that are relied upon, directly or indirectly, to enforce a security policy that governs confidentiality, integrity, and availability protections.

Sensitivity - A measure of the importance assigned to information by its owner for the purpose of denoting its need for protection.

Signature - A recognizable, distinguishing pattern associated with an attack, such as a binary string in a virus or a particular set of keystrokes used to gain unauthorized access to a system.

SMiShing (SMS phishing) - A security attack in which the user is tricked into downloading a Trojan horse, virus, or other malware onto his cellular phone or other mobile device.

Spam - Electronic junk mail or the abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages.

Split Tunneling - The process of allowing a remote user or device to establish a non-remote connection with a system and simultaneously communicate via some other connection to a resource in an external network. This method of network access enables a user to access remote devices (e.g., a networked printer) at the same time as accessing uncontrolled networks.

Spyware - Software that is secretly or surreptitiously installed into a system to gather information on individuals or organizations without their knowledge; a type of malicious code.

Supplemental Guidance - Statements used to provide additional explanatory information for security controls or security control enhancements.

System - Any organized assembly of resources and procedures united and regulated by interaction or interdependence to accomplish a set of specific functions. Note: Systems also include specialized systems such as industrial/process controls systems, telephone switching and private branch exchange (PBX) systems, and environmental control systems.

System Component - A discrete, identifiable information technology asset (hardware, software, firmware) that represents a building block of a system. System components include commercial information technology products.

System Integrity - The quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation of the system, whether intentional or accidental.

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

System Security Plan - Formal document that provides an overview of the security requirements for the system and describes the security controls in place or planned for meeting those requirements.

Tailoring - The process by which a security control baseline is modified based on: 1) the application of scoping guidance, 2) the specification of compensating security controls, if needed, and 3) the specification of organization-defined parameters in the security controls via explicit assignment and selection statements.

Threat - Any circumstance or event with the potential to adversely impact company operations (including mission, functions, image, or reputation), company assets, individuals, other organizations, or the Nation through a system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

Threat Event - An event or situation that has the potential for causing undesirable consequences or impact.

Token - Something that the claimant possesses and controls (typically a key or password) that is used to authenticate the claimant's identity.

Trojan Horse - A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program.

Trusted Computing Base - Totality of protection mechanisms within a computer system, including hardware, firmware, and software, the combination responsible for enforcing a security policy.

Trustworthy System Computer - Hardware, software and procedures that - 1) are reasonably secure from intrusion and misuse, 2) provide a reasonable level of availability, reliability, and correct operation, and 3) are reasonably suited to performing their intended functions and 4) adhere to generally accepted security procedures.

User - Individual, or a process acting on behalf of an individual, authorized to access a system.

Validation - Confirmation (through the provision of strong, sound, objective evidence) that requirements for a specific intended use or application have been fulfilled (e.g., a trustworthy credential has been presented, or data or information has been formatted in accordance with a defined set of rules, or a specific process has demonstrated that an entity under consideration meets, in all respects, its defined attributes.)

Virus - A computer program that can copy itself and infect a computer without permission or knowledge of the user. A virus might corrupt or delete data on a computer, use e-mail programs to spread itself to other computers, or even erase everything on a hard disk. See Malicious Code.

Vishing - The fraudulent practice of making phone calls or leaving voice messages purporting to be from reputable companies in order to induce individuals to reveal personal information, such as bank details and credit card numbers.

Vulnerability - Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

Whitelisting - A process used to identify software programs that are authorized to execute on a system or authorized Universal Resource Locators (URL)/websites.

Wireless Technology - Technology that permits the transfer of information between separated points without physical connection.

Worm - A self-replicating, self-propagating, self-contained program that uses networking mechanisms to spread itself. See Malicious Code.

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

Appendix A:
Useful Plans, Policies and Procedures

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

Plans you should have in place:

- Business Continuity Plans
- Contingency Plans
- Continuity of Operations Plans
- Critical Infrastructure Plans
- Crisis Communications Plan
- Disaster Recovery Plans
- Incident Response Plan
- Incident Response Testing Plan
- Occupant Emergency Plan
- Physical/Environmental Protection Plan
- Plan of Action
- Security Assessment Plan
- Security Plan
- System Security Plan

Policies and Procedures you should have:

- Access Control
- Audit and Accountability
- Configuration Management
- Configuration Planning
- Incident Response

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

- Identification and Authentication
- Information Flow Control
- Information Flow Enforcement
- Information System Maintenance
- Media Protection
- Media Sanitization and Disposal
- Mobile Code Implementation
- Password
- Personnel Security
- Physical and Environmental Protection
- Portable Media
- Risk Assessment
- Security Assessment and Authorization
- Security Awareness and Training
- Security Planning
- Separation of Duties
- System and Information Integrity
- System and Services Acquisition
- System and Communication Protection
- System Use

This publication is available free of charge from: https://doi.org/10.6028/NIST.HB.162

Attachment: NIST MEP Cybersecurity Handbook (2024-R-80 : National Institute of Standards and Technology Cybersecurity Framework)

HOLLY HILL
FLORIDA

STAFF REPORT
CITY OF HOLLY HILL, FLORIDA

City Commission
Resolution

MEETING DATE: October 22, 2024
FROM: Antoine Khoury
SUBJECT: A Resolution of the City Commission of the City of Holly Hill, Florida, Authorizing the City Manager to Execute Change Order No. 2 with Parker Mynchenberg & Associates, Inc., to Include Construction Administration Services for the 10Th Street Sewer Main Extension Project in an Amount Not to Exceed $6,075.00; Providing for Severability; and Providing for an Effective Date.
NUMBER: 2024-R-81
APPLICANT:
PLANNER:

DISCUSSION:

The City entered into an agreement for an appropriations grant to extend the sewer force main at 10th Street further west across Nova Road. To facilitate the grant, the City entered into an engineering support contract with Parker Mynchenberg & Associates to evaluate and provide the design for the approximate 1,500 linear foot run of HDPE force main pipe to a Volusia County proposed development that will have a private lift station and pump sewer to the City of Holly Hill for treatment and disposal. The proposed zoning of the subject parcel will allow for up to 134 new residential units.

Change Order # 2 provides for construction administration of the project. The original scope from Parker Mynchenberg & Associates, Inc., did not include construction administration services, inspection and project closeout. Change Order #2 in attached under “Exhibit A”.

FISCAL ANALYSIS:

The City entered into a Professional Consultant Services Agreement for Engineering/CEI Services with Parker Mynchenberg & Associates, Inc., on January 25, 2022 for a term of five (5) years with (2) (1) year renewal options.

Change Order No. 2 increases the engineering cost by $6,075.00 for the project. The project is been budgeted in account number 407-8110-580-6300 and Project Code 24-WW-07. To date the approved engineering for the project is $53,937.00. With Change Order # 2 the total engineering services will be $60,012.00. Florida State Legislative action has awarded the City funding to complete the extension of sewer services across Nova Road in the amount of $1,360,000. The State funding is anticipated to fund all of the engineering services for this project, as well as all construction.

STAFF RECOMMENDATION:

Authorize the City Manager to execute Change Order No. 2 with Parker Mynchenberg & Associates, Inc., to include construction administration, inspection and closeout service for the 10th Street Sewer Force Main Extension Project in an amount Not to Exceed $6,075.00.

COMMISSION GOALS:

Goal #1: Develop and maintain a sound and sustainable financial plan for the city that establishes sufficient reserves for all funds, ensures (whenever possible) that user fees pay for services rendered, provides a realistic capital improvement program, and encourages public/private sector partnerships and intergovernmental partnerships.

Goal #4: Provide proficient public health and safety services in terms of police and fire protection, water, storm water, waste water and solid waste management and disaster preparedness with a focus on intergovernmental collaboration, private sector partnerships, and utilization of technologies and proven innovations.

MOTION:

AUTHORIZE THE CITY MANAGER TO EXECUTE CHANGE ORDER NUMBER 2 WITH PARKER MYNCHENBERG & ASSOCIATES, INC., TO INCLUDE SURVEYING SERVICES FOR THE 10th STREET SEWER FORCE MAIN EXTENSION PROJECT IN AN AMOUNT NOT TO EXCEED $6,075.00.

ATTACHMENTS:

- Josef Grusauskas - COHH 10th Street Contract Admin (PDF)

Resolution No. 2024-81

A RESOLUTION OF THE CITY COMMISSION OF THE CITY OF HOLLY HILL, FLORIDA, AUTHORIZING THE CITY MANAGER TO EXECUTE CHANGE ORDER NO. 2 WITH PARKER MYNCHENBERG & ASSOCIATES, INC., TO INCLUDE CONSTRUCTION ADMINISTRATION SERVICES FOR THE 10TH STREET SEWER MAIN EXTENSION PROJECT IN AN AMOUNT NOT TO EXCEED $6,075.00; PROVIDING FOR SEVERABILITY; AND PROVIDING FOR AN EFFECTIVE DATE.

A RESOLUTION OF THE CITY COMMISSION OF THE CITY OF HOLLY HILL, FLORIDA, AUTHORIZING THE CITY MANAGER TO EXECUTE CHANGE ORDER NO. 2 WITH PARKER MYNCHENBERG & ASSOCIATES, INC., TO INCLUDE CONSTRUCTION ADMINISTRATION SERVICES FOR THE 10TH STREET SEWER MAIN EXTENSION PROJECT IN AN AMOUNT NOT TO EXCEED $6,075.00; PROVIDING FOR SEVERABILITY; AND PROVIDING FOR AN EFFECTIVE DATE.

WHEREAS, the City desires to extend the sewer force main at 10th Street further west across Nova Road; and

WHEREAS, the City entered into a Professional Consultant Services Agreement for Engineering/CEI Services with Parker Mynchenberg & Associates, Inc., for this project on September 26, 2023 through Resolution No 2023-R-46; and

WHEREAS, Parker Mynchenberg & Associates, Inc., has provided change order No. 2 for $6,075.00 to include construction administration, inspection and closeout services.

NOW, THEREFORE, BE IT RESOLVED BY THE CITY COMMISSION OF THE CITY OF HOLLY HILL, FLORIDA:

SECTION 1. That the City Commission of the City of Holly Hill does hereby authorize the City Manager to execute Change Order Number 2 Parker Mynchenberg & Associates, Inc., to include construction administration, inspection and closeout services for the 10th Street Sewer Main Extension Project in an amount not to exceed $6,075.00; bringing the total cost of engineering/CEI to $60,012.00.

SECTION 2. If any section or portion of a section of this Resolution proves to be invalid, unlawful, or unconstitutional, it shall not be held to invalidate or impair the validity, force, or effect of any other section or part of this Resolution.

SECTION 3. This Resolution shall take effect immediately upon its adoption.

APPROVED AND AUTHENTICATED on this 22nd day of OCTOBER, 2024.

PARKER MYNCHENBERG & ASSOCIATES, INC.

1729 Ridgewood Avenue
Holly Hill, Florida 32117
(386) 677-6891
FAX (386) 677-2114
E-Mail: info@parkermynchenberg.com

October 2, 2024

Mr. Josef Grusauskas
Deputy Director of Public Works-Utilities
City of Holly Hill
453 LPGA Blvd.
Holly Hill, FL 32117

Via email: jgrusauskas@hollyhillfl.org

Re: CITY OF HOLLY HILL – 10th STREET SEWER EXTENSION
Change Order #2 – Contract Administration
Professional Engineering Services Proposal

Dear Mr. Grusauskas:

We are pleased to offer the Professional Engineering Services for construction phase services for the above referenced project. The 10th Street sewer extension was bid on September 5th and is moving forward into construction phase. The contract administration and project certification scope is outlined below.

This Professional Services Proposal includes construction phase services.

The Scope of Work is as follows:

PART A – CONTRACT ADMINISTRATION AND PROJECT CERTIFICATION

1. Contract Administration
    a. Attend Pre-Construction Meeting
    b. Review Shop Drawings
    c. Attend Progress Meetings
    d. Pay Request Review and Approval
2. Project Close-out
    a. Review As-builts
    b. Perform Final Inspection
    c. Attend onsite walkthrough with City Staff and Contractor
    d. Create Engineering Punchlist
    e. Re-inspect Site for Completeness

PART B – MISCELLANEOUS

1. Expenses (including reproducibles, mileage, postage, etc.)

Not included in the above Scope of Work are as follows:

1. Permit application and fees (to be borne by the Owner).
2. Boundary, topographic, jurisdictional wetland, and tree survey (by a registered land surveyor).
3. Preparation of Easement Sketch and Legal Descriptions (if required).
4. Wetland Jurisdictional determination/flagging (including but not limited to vegetation mapping, on-site endangered or protected species inventory and environmental permitting associated with site plan approval, stormwater and dredge and fill permitting (mitigation plan) (if required) (PMA to provide environmental ACOE consultant, dredge and fill exhibit only). Obtaining the Army Corp of Engineer's Permit for wetlands impacts is the sole responsibility of the environmental consultant. PMA will assist with exhibits etc. However, the wetland jurisdiction impacts, mitigation plan, and obtaining the permit are NOT included in PMA's scope of work.
5. Preparation of Architectural Building Plans and Elevations. (to be prepared by Project Architect).
6. Preparation of Signage Plans (to be provided by architect or sign company).
7. Geotechnical Soil Testing (to be performed by a Geotechnical Engineer) (if required).

Attachment: Josef Grusauskas - COHH 10th Street Contract Admin (2024-R-81 : 10Th St Sewer Extension Project Change Order #2)

8. Cultural Assessment Survey and Report in response to the Division of Historical Resources (if required).
9. Preparation and assistance associated with LEED design certification.
10. Title Opinion.
11. Traffic Studies (to be prepared by Traffic Engineer) (if required).
12. Preparation of Environmental Reports (if required by the County/SJRWMD).
13. Comprehensive Plan, Rezoning Amendments and Future Land Use Modification (if required).
14. Preparation of Structural Permit Applications.
15. Preparation of Colored Renderings.
16. Preparation of a Lighting Plan including Photometric Plan and Lift Station Electrical Service and Electrical Design. (to be prepared by an Electrical Engineer).
17. Gopher Tortoise Survey or Permitting Relocation.
18. Preparation of an Endangered and Threatened Species Report.
19. Onsite Construction supervision.
20. Electrical Service or Distribution Design (by Electrical Engineer).
21. Attendance at Public Hearings, including Neighborhood Meetings, Planning Board, Redevelopment Board and City Commission Meetings unless specially included in the Scope of Work.
22. Coordination of Telephone, Gas, Cable, and Power (PMA to provide plans only to private utilities).
23. Traffic Fair Share Agreement.
24. Sanitary Pump Station Design and Permitting (if required)
25. As-Built of civil, landscaping and irrigation improvements (to be prepared by a registered land surveyor or sub-contractor as part of their contract).
26. Required bacteriological testing in conjunction with water main clearance (if required).
27. FDEP NPDES Notice of Intent (NOI) Permit (To be applied and obtained by the Contractor through the FDEP. PMA will assist but obtaining the NOI is NOT included in PMA's Scope of Work)
28. Hazardous waste cleanup/permitting.
29. Brownfield permitting.
30. Swimming Pool Design and Permitting.
31. Lot Combination or Subdivision Platting
32. City of Holly Hill Final Site Plan Approval
33. Volusia County Permitting
34. Site Plan Design
35. Landscape and Irrigation Plans
36. St. Johns River Water Management District Permitting
37. FDEP Permitting
38. Florida Department of Transportation Permitting
39. Volusia County School Concurrency Reservation
40. FAA Permitting
41. FEMA Elevation Certificates and CLOMR/LOMR Permitting
42. Design
43. Bidding Assistance
44. Permitting

Attachment: Josef Grusauskas - COHH 10th Street Contract Admin (2024-R-81 : 10Th St Sewer Extension Project Change Order #2)

I anticipate the Professional Engineering Fee associated with the above Scope of Work not to exceed the following:

PART A – CONTRACT ADMINISTRATION:	**$**	**5,875.00**
PART B – MISCELLANEOUS:	**$**	**200.00**
TOTAL:	**$**	**6,075.00**

SIX THOUSAND SEVENTY-FIVE DOLLARS AND 00/100

Please note that miscellaneous expenses such as reproducibles, mileage, postage, etc. are estimated and included in the above Scope of Work. Billing will be monthly, based on the ***Hourly Rate Schedule*** included with this proposal.

After reviewing this proposal, if it meets with your approval, please execute the ***Professional Service Agreement*** and return to me as the Notice to Proceed. Please feel free to call with any questions you may have concerning this proposal or the project in general.

Thank you for considering Parker Mynchenberg & Associates, Inc. for your Professional Engineering needs.

Yours truly,



Parker Mynchenberg, P.E., R.L.A.

Attachment: Josef Grusauskas - COHH 10th Street Contract Admin (2024-R-81 : 10Th St Sewer Extension Project Change Order #2)

PROFESSIONAL SERVICES AGREEMENT

CLIENT HEREBY REQUESTS THE PERFORMANCE OF THE SERVICES IDENTIFIED IN THE DETAILED SCOPE OF WORK.

FEE BASIS
☒ Schedule of Hourly Rates Attached
☒ Miscellaneous Expenses
☒ Lump Sum Not to Exceed Fee

PAYMENT BASIS
☒ Monthly
☐ At time of Completion
☐ Retainer Required: $ N/A

LIABILITY LIMITATION
To the maximum extent permitted by law, the Client agrees to limit the Design Professional's liability for the Client's damages to the sum of $1,000,000. or the Design Professional's fee, whichever is greater. This limitation shall apply regardless of the cause of action or legal theory pled or asserted.

SERVICE CHARGE
On all amounts not paid within 30 days from date of invoice, a service charge will be made of 1.5% per month (18% per annum). This service charge shall be applied to the total outstanding balance due.

VENUE and COST OF LITIGATION
On all amounts not paid within 30 days from the date of invoice, the Client shall be responsible for all collection costs, including but not limited to Attorney's fees. In the event of a fee dispute, venue of any litigation to resolve said dispute shall be in Volusia County, Florida. Reasonable attorney's fees and costs shall be assessed for the prevailing party against the losing party in any litigation pertaining to collection fees or costs accrued, as a result of the representation outlined by the proposal.

Work shall commence upon execution of the Professional Services Agreement.

FOR: PARKER MYNCHENBERG & ASSOCIATES, INC.

BY: _____
Parker Mynchenberg, President

DATE: 10/02/2024

FOR: THE CLIENT

BY: _____

TITLE: _____

DATE: _____

Attachment: Josef Grusauskas - COHH 10th Street Contract Admin (2024-R-81 : 10Th St Sewer Extension Project Change Order #2)

HOURLY RATE SCHEDULE

Principal Engineer	$300.00/hour
Senior Project Engineer	$250.00/hour
Landscape Architect	$250.00/hour
Project Engineer	$175.00/hour
Senior CAD Technician	$150.00/hour
CAD Technician	$130.00/hour
Administrative	$ 55.00/hour

STANDARD RATE FOR MISCELLANEOUS EXPENSES

PRINTS

24”x36”	$2.00/ea.
30”x42”	$3.00/ea.
36”x48”	$4.00/ea.
42”x60”	$6.00/ea.

REPRODUCIBLES

Mylar	$20.00/ea.

COPIES

8.5”x11”	$0.25/ea.
8.5”x14”	$0.35/ea.
11”x17”	$0.40/ea.
Color	$1.50/ea.

OTHER

Mileage	$0.75/mile
Postage	Current Rate
Phone Calls	As Billed

Attachment: Josef Grusauskas - COHH 10th Street Contract Admin (2024-R-81 : 10Th St Sewer Extension Project Change Order #2)

FEE MATRIX

Task	Description	Senior Project Engineer (PE) $ 250	Project Engineer (EI) $ 175	Senior CAD Technician $ 150	Clerical $ 55	Man Hours	Cost	Total
PART A – CONTRACT ADMINISTRATION								
1)	Attend Preconstruction Meeting	-	2	-	2	4.0	$460.00	
2)	Attend Monthly on-site meetings	6	-	-	1	7.0	$1,555.00	
3)	Shop drawing review	2	-	-	2	4.0	$610.00	
4)	Substantial and final walk-thru/punch list	2	-	-	1	3.0	$555.00	
5)	As-built review and certification	-	1	2	1	4.0	$530.00	
6)	RFI's	2	2	2	2	8.0	$1,260.00	
7)	Field Change Orders	2	2	-	1	5.0	$905.00	**$5,875.00**
PART B - MISCELLANEOUS								
1)	Expenses (including reproducibles, mileage, postage, etc.)	-	-	-	-	0.0	$200.00	**$200.00**
		14	7	4	10	35		
		$3,500.00	$1,225.00	$600.00	$550.00		$6,075.00	**$6,075.00**
							$6,075.00	

Attachment: Josef Grusauskas - COHH 10th Street Contract Admin (2024-R-81 : 10Th St Sewer Extension

HOLLY HILL
FLORIDA

STAFF REPORT
CITY OF HOLLY HILL, FLORIDA

City Commission
Resolution

MEETING DATE: October 22, 2024
FROM: Antoine Khoury
SUBJECT: A Resolution of the City Commission of the City of Holly Hill, Florida, Approving Price Agreements for the Purchase of the Fiscal Year 2024-2025 Supply of Water and Wastewater Treatment Chemicals for the Public Works Department and Authorize the City Manager to Execute Any Necessary Price Agreements; Providing for Severability; and Providing for an Effective Date.
NUMBER: 2024-R-82
APPLICANT:
PLANNER:

DISCUSSION:

The City's Public Works Department utilizes various chemicals for the treatment of water and wastewater through various procurement methods. These chemicals are designed into the operational treatment process to maintain high quality drinking water disinfection and wastewater reuse compliance.

Current City of Holly Hill Purchasing Manual:

SECTION F - SOLE SOURCE AND STANDARDIZATION PROCUREMENT POLICY 2.25 EXEMPTION FROM BIDDING PROCEDURE

Sole source or Standardization procurement is exempt from bidding procedures. The using department must submit to the Finance Department in writing for his/her approval the attempts made, or the data collected to substantiate declaring a product or service "sole source". The City Commission must approve the award of the contract if the dollar amount exceeds $50,000.

SOLE SOURCE

The following criteria must be met in order to satisfy the sole source or proprietary source requirement:

• The item is available from only one source of supply.

• The purchase is during a Public Emergency.

• Competition is deemed inadequate after solicitation or Request for Quotation.

Sole source and proprietary source purchases are exempt from competitive requirements. However, all sole source requisitions exceeding $50,000 in value will be electronically

advertised for a period of at least 7 business days. The steps to follow for sole source and proprietary source purchases are as follows:

a. The User Department/Department and the Finance Department shall attempt to locate competition. Staff will also check for piggyback contracts. If no other sources are found, the User Department/Department shall submit to the Finance Department a completed sole source/proprietary source form, indicating the requisition number.

b. A sole source or proprietary source form shall be used to justify and document the requirement. The form shall state why only one source can produce the desired results (or fulfill the specific need).

c. The Finance Department will electronically post on the City website a description of all requisitions meeting the requirements for competitive pricing per Florida Statute for a period of at least seven (7) business days after the receipt of a completed sole source form from the department.

d. The Finance Director shall review and approve or disapprove, in writing; sole source/proprietary source designation.

e. The User Department/Department shall be notified of disapproved requests and the purchase shall be made in accordance with standard procedures.

f. When the Finance Director approves a sole or proprietary source, staff shall conduct negotiations on price, delivery, and terms. The price must be determined fair and reasonable.

g. The Finance Department shall keep a log of sole/proprietary source purchases, which includes the vendor name, the amount, item description, justification, and the purchase order number.

h. For those instance that services are needed involving multiple years (i.e. maintenance of equipment, warranty, etc.) the request must be combined to capture the project, as a whole, and the proper approval must be obtained.

STANDARDIZATION

Standardization is the process of examining characteristics and needs for items of similar end usage and developing a single specification that will satisfy the need for most or all purchases for that purpose. Proprietary purchases (usually components) maintain a degree of continuity to the original or existing decor, equipment, or programs.

Where standardization is determined to be desirable by the City, the purchase of materials, supplies and equipment and certain contractual services may be made by negotiation.

Compatibility to existing equipment will be an acceptable justification for waiver of bidding procedures provided the item meets the other criteria within the definition of sole source item (i.e.; available from only one source and only item that will produce the desired results).

Sole Source Vendors

In some cases, standardization is in the best interest of the City due to additional costs for product testing, product storage, availability or other factors such as a demonstrated chemical

performance with the City's treatment process application equipment and dosage rate. This is the case with: FBS 10910 is a water-soluble polymer utilized in the wastewater treatment plant to enhance settlement, Aqua Gold, a blended phosphate product utilized stabilize drinking water and Praestol K260FL, a water-soluble product specifically designed to thicken sludge in the belt press for disposal and MircoC 2000 a carbon supplement to enhance the wastewater treatment process f or sole source pricing as they have been on-site tested and demonstrated to maintain treatment compliance.

These company's sole source letter and sole source justification forms are attached under Exhibits A, B, C & D respectively.

FISCAL ANALYSIS:

The expenditures related to the purchase of chemicals are fully budgeted in the utilities budget covering the water and wastewater divisions. The actual amount of expenditures for the above chemicals will vary with use throughout the year as required by the treatment process. Funds are budgeted through the respective operating supplies account for the water and wastewater accounts. Specifically,

1) The purchase of FBS 10910 (polymer) for the wastewater division account 400-3020-535-5201 in the amount of $49,140.00/yr.

2) The purchase of Aqua Gold for the water division account 400-3010-535-5201 in the amount of $28,187.00/yr.

3) The purchase of Praestol K260FL (polymer) for the wastewater division account 400-3020-535-5201 in the amount of $49,140.00/yr.

4) The Purchase of MicroC 2000 for the wastewater division account 400-3020-535-5201 at $79,000.00/yr.

STAFF RECOMMENDATION:

Approve price agreements for the purchase of Fiscal Year 2024-2025 supply of water and wastewater treatment chemicals for the Public Works Department and authorize the City Manager to execute necessary price agreements.

COMMISSION GOAL:

Goal #1: Develop and maintain a sound and sustainable financial plan for the city that establishes sufficient reserves for all funds, ensures (whenever possible) that user fees pay for services rendered, provides a realistic capital improvement program, and encourages public/private sector partnerships and intergovernmental partnerships.

Goal #4: Provide proficient public health and safety services in terms of police and fire protection, water, storm water, waste water and solid waste management and disaster preparedness with a focus on intergovernmental collaboration, private sector partnerships, and utilization of technologies and proven innovations.

MOTION:

APPROVING PRICE AGREEMENTS FOR THE PURCHASE OF THE FISCAL YEAR 2023-2024 SUPPLY OF WATER AND WASTEWATER TREATMENT CHEMICALS FOR THE PUBLIC WORKS DEPARTMENT AND AUTHORIZING THE CITY MANAGER TO EXECUTE ANY NECESSARY PRICE AGREEMENTS.

ATTACHMENTS:

- Exhibit A - Sole Source FBS 10910 Polymer.pdf (PDF)
- Exhibit B - Sole Source Aqua Gold Corrosion Inhibitior.pdf (PDF)
- Exhibit C - Sole Source Praestrol K 260 FL.pdf (PDF)
- Exhibit D - Sole Source MicroC 2000 carbon supplement (PDF)

Resolution No. 2024-82

A RESOLUTION OF THE CITY COMMISSION OF THE CITY OF HOLLY HILL, FLORIDA, APPROVING PRICE AGREEMENTS FOR THE PURCHASE OF THE FISCAL YEAR 2024-2025 SUPPLY OF WATER AND WASTEWATER TREATMENT CHEMICALS FOR THE PUBLIC WORKS DEPARTMENT AND AUTHORIZE THE CITY MANAGER TO EXECUTE ANY NECESSARY PRICE AGREEMENTS; PROVIDING FOR SEVERABILITY; AND PROVIDING FOR AN EFFECTIVE DATE.

A RESOLUTION OF THE CITY COMMISSION OF THE CITY OF HOLLY HILL, FLORIDA, APPROVING PRICE AGREEMENTS FOR THE PURCHASE OF THE FISCAL YEAR 2024-2025 SUPPLY OF WATER AND WASTEWATER TREATMENT CHEMICALS FOR THE PUBLIC WORKS DEPARTMENT AND AUTHORIZE THE CITY MANAGER TO EXECUTE ANY NECESSARY PRICE AGREEMENTS; PROVIDING FOR SEVERABILITY; AND PROVIDING FOR AN EFFECTIVE DATE.

WHEREAS, the City of Holly Hill is in need of chemicals for water and wastewater treatment; and

WHEREAS, the City has secured pricing agreements utilizing various procurement methods permitted under the City's purchasing guidelines; and

WHEREAS, The City Purchasing Administrator advertised the products for purchase pursuant to Florida Statute 287.057(5)(c), for a period of seven (7) business days. and

WHEREAS, By Policy 2.24 section F of the Holly Hill purchasing policy manual; "Standardization procurement is exempt from bidding procedures"; and

WHEREAS, the City Commission approves the price agreements for the purchase of Fiscal Year 2024-2025 supply of water and wastewater treatment chemicals for the Public Works Department.

NOW, THEREFORE, BE IT RESOLVED BY THE CITY COMMISSION OF THE CITY OF HOLLY HILL, FLORIDA:

SECTION 1. That the City Commission does hereby approve price agreements for the purchase of the Fiscal Year 2024-25 supply of water and wastewater treatment chemicals for the Public Works Department and authorizes City Manager to execute any necessary price agreements.

SECTION 2. SEVERABILITY. If any section or portion of a section of this Resolution

proves to be invalid, unlawful, or unconstitutional, it shall not be held to invalidate or impair the validity, force, or effect of any other section or part of this Resolution.

SECTION 3. EFFECTIVE DATE. This Resolution shall take effect immediately upon its adoption.

APPROVED AND AUTHENTICATED on the 22nd day of OCTOBER, 2024.

City of Holly Hill

Finance Department
1065 Ridgewood Ave.
Holly Hill, FL 32117

SOLE SOURCE JUSTIFICATION

TO: Finance Department	**FROM:** _____ **REQUISITION #:** _____
Subject - Purchase of: Paestrol K 260 (wastewater polymer)	
Requested Supplier Contact: Chelsea Vaughan-Burns Company: Solenis Address: 2475 Pinnacle Dr.	City, State, Zip: Wilmington, DE 19803 Phone: 866-337-1533 Estimated Cost: $ 49,140.00

Statement of Need: My recommendation for sole source is based upon an objective review of the product/service being required and appears to be in the best interest of the City. I know of no conflict of interest on my part or involved in any way with this request. No gratuities, favors or compromising actions have taken place. Neither has my personal familiarity with particular brands, types of equipment, materials or firms been a deciding influence on my request to sole source this purchase when there are other known suppliers to exist.

Sole Source Justification: Mark those that apply.

☐ 1. Sole source request is for the original manufacturer or provider; there are no regional distributors. (Attach the manufacturers written certification that no regional distributors exist. Item 4 must also be checked).

■ 2. Sole source request is for the only area distributor of the original manufacturer or provider. (Attach the manufacturers -not the distributors - written certification that identifies all regional distributors. Item 4 also must be checked).

☐ 3. The parts/equipment are not interchangeable with similar parts of another manufacturer. (Explain in comments or separate memorandum).

■ 4. This is the only known item or service that will meet the specialized needs of this department or perform the intended function. (Attach memorandum with details of specialized function or application).

☐ 5. The parts/equipment are required from this source to facilitate maintenance standardization. (Attach memorandum describing the basis for the standardization request).

☐ 6. None of the above applies. A detailed explanation and justification for this sole source request is contained in the attached memorandum.

Division Head Signature: _____ Date: 10-2-24

Department Head Signature: Antoine Ithomell Date: 10-2-24

Comments: Justification # 4 -Paestrol K 260 is the only on-site tested polymer to maintain wastewater plant permit compliance.

Finance Approval: _____ Date: _____

City Manager Approval (if required): _____ Date: _____

Attachment: Exhibit A - Sole Source FBS 10910 Polymer.pdf [Revision 1] (2024-R-82 : Treatment Plant Chemicals)

SOLENIS
Strong bonds. Trusted solutions.

Mr. John R. Dally
Chief Wastewater Operator
Dept. of Public Works
453 LPGA Blvd.
Holly Hill, FL 32117

Dear Mr. Dally,

Solenis LLC is a major global producer of water treatment polymers, including both dry and emulsion wastewater flocculants, dispersants, selected antiscalants and other innovative products. Solenis is the sole source of manufacture for PRAESTOL K 260 FL as sold to the City of Holly Hill, FL. No company other than Solenis may manufacture Praestol.

PRAESTOL© is made at the manufacturing plant located at:

SOLENIS LLC
2401 Doyle Street
Greensboro, NC 27406

Please feel free to contact me if you have any questions.

Sincerely,

Chelsea Vaughan-Burns
Business Support Analyst

Attachment: Exhibit A - Sole Source FBS 10910 Polymer.pdf [Revision 1] (2024-R-82 : Treatment Plant Chemicals)

SOLENIS
Strong bonds. Trusted solutions.

solenis.com

Chelsea Vaughan-Burns
Phone: 302-502-0802
Email: cvaughanburns@solenis.com

September 21, 2024

Mr. John Dally
City of Holly Hill
453 LPGA Boulevard
Holly Hill, FL 32117

Re: Praestol K 260 FL Price Extension

Dear Mr. Dally,

Solenis LLC is please to extend the current price for a twelve-month period as follows:

PRODUCT NAME	PRICE/LB
Praestol K260FL	$2.10

- FOB & Shipping: Delivered/Destination Shipping Included
- Terms: Net 30
- Packaging: 55 gallon drums
- Period: October 1, 2024 –September 30, 2025
- All remaining terms and conditions are the same.

If you have any questions, please contact Ash Sanogrot, your sales representative. We value your business and look forward to another successful year.

Sincerely,

You Solenis Team

Attachment: Exhibit A - Sole Source FBS 10910 Polymer.pdf [Revision 1] (2024-R-82 : Treatment Plant Chemicals)

City of Holly Hill

Finance Department
1065 Ridgewood Ave.
Holly Hill, FL 32117

SOLE SOURCE JUSTIFICATION

TO: Finance Department	**FROM:** _____ **REQUISITION #:** _____
Subject - Purchase of: Aqua Gold Corrosion Inhibitor	
Requested Supplier Contact: Katherine Godwin Company: Dave Symonds & Associate, Inc Address: 26730 Emeralda Island Rd	City, State, Zip: Leesburg, FL 34788 Phone: 352-787-0823 Estimated Cost: $ 28,187.00

Statement of Need: My recommendation for sole source is based upon an objective review of the product/service being required and appears to be in the best interest of the City. I know of no conflict of interest on my part or involved in any way with this request. No gratuities, favors or compromising actions have taken place. Neither has my personal familiarity with particular brands, types of equipment, materials or firms been a deciding influence on my request to sole source this purchase when there are other known suppliers to exist.

Sole Source Justification: Mark those that apply.

☐ 1. Sole source request is for the original manufacturer or provider; there are no regional distributors. (Attach the manufacturers written certification that no regional distributors exist. Item 4 must also be checked).

■ 2. Sole source request is for the only area distributor of the original manufacturer or provider. (Attach the manufacturers -not the distributors - written certification that identifies all regional distributors. Item 4 also must be checked).

☐ 3. The parts/equipment are not interchangeable with similar parts of another manufacturer. (Explain in comments or separate memorandum).

■ 4. This is the only known item or service that will meet the specialized needs of this department or perform the intended function. (Attach memorandum with details of specialized function or application).

☐ 5. The parts/equipment are required from this source to facilitate maintenance standardization. (Attach memorandum describing the basis for the standardization request).

☐ 6. None of the above applies. A detailed explanation and justification for this sole source request is contained in the attached memorandum.

Division Head Signature: _____ Date: 10-2-24

Department Head Signature: 10-2-24 AEK Date: _____

Comments: Justification # 4 - Aqua Gold is the only on-site tested corrosion inhibitor to maintain water plant permit compliance to meet State and Federal Lead and Copper Rule.

Finance Approval: _____ Date: _____

City Manager Approval (if required): _____ Date: _____

Attachment: Exhibit B - Sole Source Aqua Gold Corrosion Inhibitior.pdf [Revision 1] (2024-R-82 : Treatment Plant Chemicals)

DAVE SYMONDS & ASSOCIATES, INC.

36730 EMERALDA ISLAND RD.
LEESBURG, FLORIDA 34788
(352) 787-0340 or 1-800-226-0340
FAX (352) 787-0823

September 4, 2024

Town of Holly Hill

453 LPGA Blvd

Holly Hill, FL 32117

Ref – 2025 Aqua Gold 170 price quote

Att: Jeff Jacobson – Chief Water Plant Operator

Mr. Jacobson,

The price for the Aqua Gold 170 at your location in Holly Hill is $15.90 - .37 = $15.53 per gallon. This price is good for October 1,2024 to October 1,2025.

Beginning in March of 2025 we will assess the price every three months. We do not anticipate a price increase however in the event of one, your price increase would not exceed 20% for the next fiscal year.

Please let me know if you need any further information.

We appreciate your business.

Thank you,

Kathrine Godwin

Kathrine Godwin

Attachment: Exhibit B - Sole Source Aqua Gold Corrosion Inhibitior.pdf [Revision 1] (2024-R-82 : Treatment Plant Chemicals)

WATER SOLUTIONS UNLIMITED

Symonds & Associates
36730 Emeralda Island Road
Leesburg, FL. 34788
Attn: Fred Symonds & Kathy Godwin

June 28, 2024

Dear Fred and Kathy:

Sole Source Agreement

Per your request, I have updated this '*Sole Source Agreement*' which confirms that Symonds & Associates has sole rights to the distribution of our AQUAGOLD and AQUAFRESH products, within the State of Florida 2024 AND 2025. This letter will serve as confirmation of our agreement for Symonds & Associates being the sole source of the above stated product lines (manufactured by Water Solutions Unlimited, Inc. - Mersch Consulting, Inc.) throughout the State of Florida.

The great relationship that we have established with your company, is excellent and I look forward to working with everyone at Symonds & Associates throughout the future. I will supply the technical support necessary for your efforts throughout this part of the country and I expect this agreement will continue to provide for many more years of successful water treatment for numerous communities throughout the State of Florida.

Sincerely:

Mike Ricks
President
Water Solutions Unlimited, Inc.
8824 Union Mills Drive
Camby, IN 46113

Cell: 317-339-6639, office: 317-736-6868
e-mail:mike.ricks@getwsu.com

Attachment: Exhibit B - Sole Source Aqua Gold Corrosion Inhibitior.pdf [Revision 1] (2024-R-82 : Treatment Plant Chemicals)

City of Holly Hill

Finance Department
1065 Ridgewood Ave.
Holly Hill, FL 32117

SOLE SOURCE JUSTIFICATION

TO: Finance Department	**FROM:** _____ **REQUISITION #:** _____
Subject - Purchase of: FBS 10910 (wastewater polymer)	
Requested Supplier Contact: Boyd Stanly Company: Polydynemic Address: 1 Chemical Plant Rd	City, State, Zip: Riceboro, GA 31323 Phone: 941-961-3998 Estimated Cost: $ 49,140.00

Statement of Need: My recommendation for sole source is based upon an objective review of the product/service being required and appears to be in the best interest of the City. I know of no conflict of interest on my part or involved in any way with this request. No gratuities, favors or compromising actions have taken place. Neither has my personal familiarity with particular brands, types of equipment, materials or firms been a deciding influence on my request to sole source this purchase when there are other known suppliers to exist.

Sole Source Justification: Mark those that apply.

☐ 1. Sole source request is for the original manufacturer or provider; there are no regional distributors. (Attach the manufacturers written certification that no regional distributors exist. Item 4 must also be checked).

☒ 2. Sole source request is for the only area distributor of the original manufacturer or provider. (Attach the manufacturers -not the distributors - written certification that identifies all regional distributors. Item 4 also must be checked).

☐ 3. The parts/equipment are not interchangeable with similar parts of another manufacturer. (Explain in comments or separate memorandum).

☒ 4. This is the only known item or service that will meet the specialized needs of this department or perform the intended function. (Attach memorandum with details of specialized function or application).

☐ 5. The parts/equipment are required from this source to facilitate maintenance standardization. (Attach memorandum describing the basis for the standardization request).

☐ 6. None of the above applies. A detailed explanation and justification for this sole source request is contained in the attached memorandum.

Division Head Signature: _____ Date: 10-2-24

Department Head Signature: Antoine D Khoury Date: 10-2-24

Comments: Justification # 4 -FBS 10910 is the only on-site tested polymer to maintain wastewater plant permit compliance.

Finance Approval: _____ Date: _____

City Manager Approval (if required): _____ Date: _____

Attachment: Exhibit C - Sole Source Praestrol K 260 FL.pdf [Revision 1] (2024-R-82 : Treatment Plant Chemicals)

SNF
WATER SCIENCE

polydyneinc.com

September 19, 2024

John R. Dally, Chief WWTP Operator
Department of Public Works
City of Holly Hill
453 LPGA Boulevard
Holly Hill, FL 32117

SUBJECT: Sole Source Declaration

Dear Mr. Dally:

Please accept this letter as a sole source declaration to the City of Holly Hill that the polymer utilized by the City of Holly Hill, FBS 10910 can only be provided by Polydyne Inc. for the City's use.

Polydyne Inc. is the largest supplier of water-soluble polymers to the U.S. municipal water and wastewater treatment market. We have the widest range of domestically produced polymer chemistries available in the U.S. Our sales team is comprised of 28 representatives strategically located throughout the U.S., many of whom are degreed engineers.

Thank you for your business. If you have any questions or need additional information, please contact Chris Cherp, Sr. Technical Sales Representative, at (941) 961-3998. Orders may be placed online at: www.polydyneinc.com or through our Customer Service Department. Your Customer Service Representative is Karin Tanner. You can reach Ms. Tanner by calling (800) 848-7659, Ext. 8748, or by email to ktanner@snf.com.

Best regards,

Boyd Stanley
Sr. Vice-President

Attachment: Exhibit C - Sole Source Praestrol K 260 FL.pdf [Revision 1] (2024-R-82 : Treatment Plant Chemicals)

SNF
WATER SCIENCE

polydyneinc.com

September 6, 2024

Mr. John Dally
Chief WWTP Operator
City of Holly Hill
453 LPGA Boulevard
Holly Hill, FL 32117
386.248.9463

Subject: City of Holly Hill Polymer Quote

Dear Mr. Dally,

Polydyne Inc. is pleased to provide a price quote to the City of Holly Hill for the following polymer. The quote is as follows, delivered and is good through 9/30/2025:

Product	Price	Package
Clarifloc® FBS 10910	$1.80/LB.	Drum

To place your order please call or email Karin Tanner our customer service representative at 912.884.8748 or ktanner@snf.com. Should you have any questions regarding this correspondence, please feel free to contact me at 941.961.3998.

Best regards,

Chris Cherp
Sr. Technical Sales Representative
Ccherp@PolydyneInc.com

Attachment: Exhibit C - Sole Source Praestrol K 260 FL.pdf [Revision 1] (2024-R-82 : Treatment Plant Chemicals)

City of Holly Hill

Finance Department
1065 Ridgewood Ave.
Holly Hill, FL 32117

SOLE SOURCE JUSTIFICATION

TO: Finance Department	**FROM:** _____ **REQUISITION #:** _____
Subject - Purchase of: MicroC 2000 - Wastewater Carbon Supplement	
Requested Supplier Contact: Evan Brown Company: Environmental Operting Solutions, Inc Address: 53 Portside Dr.	City, State, Zip: Pocasset, MA 02559 Phone: 866-642-7621 Estimated Cost: $ 79,000.00

Statement of Need: My recommendation for sole source is based upon an objective review of the product/service being required and appears to be in the best interest of the City. I know of no conflict of interest on my part or involved in any way with this request. No gratuities, favors or compromising actions have taken place. Neither has my personal familiarity with particular brands, types of equipment, materials or firms been a deciding influence on my request to sole source this purchase when there are other known suppliers to exist.

Sole Source Justification: Mark those that apply.

☐ 1. Sole source request is for the original manufacturer or provider; there are no regional distributors. (Attach the manufacturers written certification that no regional distributors exist. Item 4 must also be checked).

■ 2. Sole source request is for the only area distributor of the original manufacturer or provider. (Attach the manufacturers -not the distributors - written certification that identifies all regional distributors. Item 4 also must be checked).

☐ 3. The parts/equipment are not interchangeable with similar parts of another manufacturer. (Explain in comments or separate memorandum).

■ 4. This is the only known item or service that will meet the specialized needs of this department or perform the intended function. (Attach memorandum with details of specialized function or application).

☐ 5. The parts/equipment are required from this source to facilitate maintenance standardization. (Attach memorandum describing the basis for the standardization request).

☐ 6. None of the above applies. A detailed explanation and justification for this sole source request is contained in the attached memorandum.

Division Head Signature: _____ Date: 10-3-24

Department Head Signature: Antoine I Khoury Date: 10-3-24

Comments: Justification # 4 - MicroC 2000, a wastewater treatment carbon supplement has been field tested ton-site to meet permitted wastewater treatment compliance requirements. The supplements are provided in totes for portable application.

Finance Approval: _____ Date: _____

City Manager Approval (if required): _____ Date: _____

Attachment: Exhibit D - Sole Source MicroC 2000 carbon supplement [Revision 1] (2024-R-82 : Treatment Plant Chemicals)

Environmental Operting Solutions, Inc.
53 Portside Dr Pocasset, MA 02559
866-642-7621 • info@microc.com

Evan Brown
Environmental Operating Solutions, Inc. (EOSi)
53 Portside Drive
Pocasset, MA 02559

October 3, 2024

Hawkins, Inc.
Hawkins Water Treatment Group
2263 Clark Street
Apopka, FL 32703

To whom it may concern,

This letter is to inform you that Environmental Operating Solutions, Inc. (EOSi), a corporation with principal address at 53 Portside Drive, Pocasset, MA 02559, is the sole manufacturer of the MicroC® 2000 supplemental carbon product. In the state of Florida, the sole supplier of less than bulk packaging is Hawkins, Inc.

Please feel free to contact me at (336) 207-5616 if you have any questions or require additional information.

Sincerely,

Evan Brown
Southeast Territory Manager

Attachment: Exhibit D - Sole Source MicroC 2000 carbon supplement [Revision 1] (2024-R-82 : Treatment Plant Chemicals)

HAWKINS, INC.
HAWKINS WATER TREATMENT GROUP

October 3, 2024

To: City of Holly Hill

ATTN: Josef Grusauskas

Shipment: This quote is in reference to MicroC 2000 70%

QTY:	Description:	Unit Price	Total
1	*MicroC 2000 70%*	*$7.11/ga*	*$7.11/ga*

Pricing is quoted through **9/30/2025**

Demurrage fees may apply

Delivery lead times may vary depending on availability in your area

The above pricing does not include any delivery fees or taxes if applicable

We understand that in the Municipal Industry, flows change and emergencies do occur that are unpreventable. We can ensure that we will handle any emergency as they occur. We are available 24/7 via 1-800-330-1369.

TERMS: Net 30 days from delivery. Our pricing does not include any additional installation or sales/excise taxes that may apply.

QUOTATION/PROPOSAL

This quotation constitutes an offer to furnish the items listed subject to; terms and conditions stated hereon; receipt of your purchase order by Hawkins Water Treatment Group, Inc.; and written acceptance of your order by Hawkins Water Treatment Group, Inc. and/or the manufacturer(s) involved as follows;

Attachment: Exhibit D - Sole Source MicroC 2000 carbon supplement [Revision 1] (2024-R-82 : Treatment Plant Chemicals)

HOLLY HILL
FLORIDA

STAFF REPORT
CITY OF HOLLY HILL, FLORIDA

City Commission
Resolution

MEETING DATE: October 22, 2024
FROM: Antoine Khoury
SUBJECT: **A Resolution of the City Commission of the City of Holly Hill, Florida, Approving the Repair of the Sewer Main at 2Nd Street and Carswell Avenue by Black Sands Development, LLC, at a Cost of $110,206.90 and Authorize the City Manager to Execute the Same; Providing for Severability; and Providing for an Effective Date.**
NUMBER: 2024-R-83
APPLICANT:
PLANNER:

DISCUSSION:

In August of 2024, a depression formed at 2nd Street and Carswell Avenue that was due to a gravity sewer main break. In 2022 the same main had another break in different location. These breaks will continue forward every couple of years. Public Works has requested that the main be replaced from manhole to manhole (115 LF) to ensure this break will not recur in the future. The cost for this sewer main replacement is $110,206.90.

FISCAL ANALYSIS:

The City entered into an agreement for utility infrastructure construction and restoration services with Black Sands Development Group, LLC as the Primary Contractor on February 24, 2024 for a term of (1) year with (4) (1) year extension options.

The cost for this authorization is $110,206.90 and the funding is available in project 25-WW-04 in account # 407-8110-580-6300.

STAFF RECOMMENDATION:

That the City Commission approve the Resolution as submitted by staff accepting the task order with Black Sands Development Group, LLC to replace the sewer main and authorize the City Manager to execute the same.

COMMISSION GOAL:

Goal #1: Develop and maintain a sound and sustainable financial plan for the city that establishes sufficient reserves for all funds, ensures (whenever possible) that user fees pay for services rendered, provides a realistic capital improvement program, and encourages

public/private sector partnerships and intergovernmental partnerships.

Goal #2: Enhance City aesthetics through beautification and maintenance of city property and public rights of way, consistent enforcement of zoning and property maintenance codes, and development of reasonable design standards and a corresponding process which is applicable to all new developments and business improvements in the city.

Goal #4: Provide proficient public health and safety services in terms of police and fire protection, water, storm water, waste water and solid waste management and disaster preparedness with a focus on intergovernmental collaboration, private sector partnerships, and utilization of technologies and proven innovations.

MOTION:

APPROVE THE TASK ORDER WITH BLACK SANDS DEVELOPMENT GROUP, LLC FOR THE WASTEWATER REPAIR AT 2ND STREET AND CARSWELL AVENUE FOR $110,206.90 AND AUTHORIZE THE CITY MANAGER TO EXECUTE THE PURCHASE FOR THE CONSTRUCTION SERVICES.

ATTACHMENTS:

- Black Sands - Signed Vender Services Agreement 2024 (PDF)
- Black Sands B?id (PDF)
- 2nd Street at carswell (JPG)

Resolution No. 2024-83

A RESOLUTION OF THE CITY COMMISSION OF THE CITY OF HOLLY HILL, FLORIDA, APPROVING THE REPAIR OF THE SEWER MAIN AT 2ND STREET AND CARSWELL AVENUE BY BLACK SANDS DEVELOPMENT, LLC, AT A COST OF $110,206.90 AND AUTHORIZE THE CITY MANAGER TO EXECUTE THE SAME; PROVIDING FOR SEVERABILITY; AND PROVIDING FOR AN EFFECTIVE DATE.

A RESOLUTION OF THE CITY COMMISSION OF THE CITY OF HOLLY HILL, FLORIDA, APPROVING THE REPAIR OF THE SEWER MAIN AT 2ND STREET AND CARSWELL AVENUE BY BLACK SANDS DEVELOPMENT, LLC AT A COST OF $110,206.90 AND AUTHORIZE THE CITY MANAGER TO EXECUTE THE SAME; PROVIDING FOR SEVERABILITY; AND AN EFFECTIVE DATE.

WHEREAS, a depression in the road has happened multiple times in the area of 2nd Street and Carswell Avenue; and

WHEREAS, city employees have repaired the sewer main two times; and

WHEREAS, city staff believes the breaks will continue until the sewer main is replaced; and

WHEREAS, the City entered into a contract with Black Sands Development Group, LLC for infrastructure construction and restoration service on February 24, 2024; and

WHEREAS, Black Sands Development Group, LLC has submitted a bid task for this repair in the amount of $110,206.90 for the repair of the sewer main; and

WHEREAS, staff recommends the approval of the task order for the repair of the sewer main.

NOW, THEREFORE, BE IT RESOLVED BY THE CITY COMMISSION OF THE CITY OF HOLLY HILL, FLORIDA:

SECTION 1. That the City Commission of the City of Holly Hill approve the task order for the repair of the sewer main in the amount of $110,206.90 and authorize the City Manager to execute the same.

SECTION 2. SEVERABILITY. If any section or portion of a section of this Resolution proves to be invalid, unlawful, or unconstitutional, it shall not be held to invalidate or impair the validity, force, or effect of any other section or part of this Resolution.

SECTION 3. EFFECTIVE DATE. This Resolution shall take effect immediately upon its adoption.

APPROVED AND AUTHENTICATED on this 22nd day of OCTOBER, 2024.

VENDOR SERVICES AGREEMENT
Utility Infrastructure Construction and Restoration
Services RFP#24-PW-02

THIS AGREEMENT is made and entered into this 22nd day of Feb, 2024, by and between Black Sands Development Group, PLLC, duly authorized to conduct business in the State of Florida and whose address is 994 Derbyshire Rd, Daytona, FL 32117, hereinafter, called "CONTRACTOR" and the **CITY OF HOLLY HILL**, a political subdivision of the State of Florida, whose address is 1065 Ridgewood Ave, Holly Hill, FL 32117, hereinafter called "CITY".

SECTION 1. AGREEMENT. The terms of this Agreement, together with the incorporation of the terms and conditions of the Request for Proposal (RFP #24-PW-02), and any exhibits, schedules and attachments hereto, and any and all amendments relating to same, and any and all submittals from CONTRACTOR, constitute the entire Agreement between CITY and CONTRACTOR. This Agreement is the final, complete and exclusive expression of the terms and conditions of the parties' Agreement. Any and all prior agreements, representations, negotiations, and understandings made by the parties, oral or written, expressed or implied, are hereby superseded and merged herein.

SECTION 2. TERM OF AGREEMENT. The term of this Agreement shall be for one (1) year from the date of award with four (4) additional one (1) year extension options. Renewal options may be exercised at the discretion of the City Manager based on performance of the company and adherence to the terms and conditions set forth in the RFP documents. The City Manager retains the sole right to determine whether the renewal option shall be granted.

SECTION 3. COMPENSATION. For Services rendered, the CITY shall pay the CONTRACTOR a lump-sum fee, including or excluding reimbursable expenses as mutually agreed upon. Unless otherwise agreed in a Scope of Services, the CONTRACTOR will invoice the City monthly based upon the CONTRACTOR's estimate of the portion of the total Services actually completed at the time of billing.

SECTION 4. NOTICES. Whenever either party desires to give notice unto the other, it must be given by written notice, sent by registered or certified United States mail, return receipts requested, addressed to the party for whom it is intended at the place last specified. The place for giving of notice shall remain such until it shall have been changed by written notice in compliance with the provisions of this Section. For the present, the parties designate the following as the respective places for giving of notice, to-wit:

For City:
Valerie Manning, City Clerk
City of Holly Hill
1065 Ridgewood Ave.
Holly Hill, FL 32117
(386)248-9441

For Contractor:
Allison R Worsham, Operations Dir. (Name, Title)
Black Sands Development Group. (Company)
994 Derbyshire Road (Address)
Daytona Beach, FL 32117 (City, State, Zip)
(386)944-9351 (Phone)

Attachment: Black Sands - Signed Vender Services Agreement 2024 (2024-R-83 : 2Nd St and Carswell Ave Depression in Road)

SECTION 5. RIGHTS AT LAW RETAINED. The rights and remedies of CITY, provided for under this Agreement, are in addition and supplemental to any other rights and remedies provided by law.

SECTION 6. CONTROLLING LAW, VENUE, ATTORNEY'S FEES. This Agreement is to be governed, construed, and interpreted by, through and under the laws of Florida. Venue for any litigation between the parties to this Agreement shall be in the County of Volusia, Florida and any trial shall be non- jury. The prevailing party in any litigation arising from or related to this Agreement shall be reimbursed reasonable attorney fees and costs, including all fees and costs of an appeal.

SECTION 7. MODIFICATIONS TO AGREEMENT. This Agreement and any exhibits, amendments and schedules may only be amended, supplemented, modified or canceled by a written instrument duly executed by the parties hereto of equal dignity herewith.

SECTION 8. SEVERABILITY. If, during the term of this Agreement, it is found that a specific clause or condition of this Agreement is illegal under federal or state law, the remainder of the Agreement not affected by such a ruling shall remain in force and effect.

SECTION 9. WAIVER OF JURY TRIAL. THE CITY AND CONSULTANT HAVE SPECIFICALLY WAIVED THE RIGHT TO A JURY TRIAL CONCERNNG ANY DISPUTES WHICH MAY ARISE CONCERNING THIS AGREEMENT.

SECTION 10. NON-WAIVER. No indulgence, waiver, election or non-election by CITY under this Agreement shall affect CONSULTANT's duties and obligations hereunder.

IN WITNESS WHEREOF, the parties hereto have made and executed this Agreement on the date written above for execution by CITY.

WITNESSES:

CITY OF HOLLY HILL

Joseph Forte, City Manager
Dated: 3-13-2024

Valerie Manning
City Clerk, CMC

WITNESSES:
By:

FIRMS
Black Sands Development Group
Allison R. Worsham, Operations Director

Dated: Feb 22nd 2024

Attachments: A. RFP #24-PW-02
B. Firm Response to RFP

Approved by the City Commission of the City of Holly Hill at a meeting held on this 12th day of March, 2024 under Agenda Item No. 5(1).

Attachment: Black Sands - Signed Vender Services Agreement 2024 (2024-R-83 : 2Nd St and Carswell Ave Depression in Road)

25WW04

Black Sands - ITEMIZED BID WORKSHEET FORM 2024

RFP # 24-PW-02 For UTILITY INFRASTRUCTURE & SITE RESTORATION SERVICES TASK ORDERS

Bidder to complete Maximum Unit Price Item prices. TASK: 2nd & Carswell Depression - REV
Future TBA Task orders will be issued based actual "Quanity" and "Unit Price Item" costs for each project and restoration services as funded by City the budget.

Line Item Pricing to Develop Project & Restoration Task Orders
Note: If not bidding on an item, indicate "No Bid" in Unit Price cell.
Note: If no cost for item, indicate $0.00 or "N/C" (no charge) in Unit Price cell.
Note: Unit Prices are "Maximum Unit Prices" for the term of the contract. Units price may be less but not more based on Work Order Assignments which includes subcontractor items such as directional drilling and dewatering services. (Contractors are encouraged to subcontract specialty services not performed in-house to complete unit pricing.)

Pay Item	Descriptions	Unit	Qty	Maximum Unit Price $'s	Extended Price $'s for Task Order
1.00 Mobilization, Traffic Control and Project Documentation					
1.01	Mobilization/Demobilization (Not exceed 10% of task order)	%	0.10	10%	Moved to bottom
1.02	Maintenance of Traffic (Not to exceed 5% of task order)	%	0.05	5%	Moved to bottom
1.03	Arrow Board / Advance Warning Flashing	ED	0	$ 65.00	$ -
1.04	Portable Changeable Message Sign, Temp.	ED	0	$ 75.00	$ -
1.05	Pre Construction Video of Work Area	EA	0	$ 1,200.00	$ -
1.06	Utility System Record Drawings	EA	0	$ 3,700.00	$ -
1.07	FDEP Partial and Final Clearance Testing/Certifications	EA	0	$ 2,500.00	$ -
1.08	FDEP Final Clearance Testing/Certifications	EA	0	$ 1,006.43	$ -
1.09	Utility Survey and Layout Staking	EA	0	$ 6,800.00	$ -
1.09	FL/Federal Funding Req. (Not exceed 5% of task order)	%	0.05	5%	Moved to bottom
				Subtotal-Section 1	**0**

Pay Item	Descriptions	Unit	Qty	Maximum Unit Price $'s	Extended Price $'s for Task Order
2.00 General Site Work and Site Protection					
2.01	Sediment Barrier (Silt Fence)	LF	0	$ 5.25	$ -
2.02	Inlet Protection System	EA	0	$ 365.00	$ -
2.03	Clearing and Grubbing	SY	0	$ 15.00	$ -
2.04	Removal of Existing Structure	SF	0	$ 150.00	$ -
2.05	Removal of Existing Concrete Pavement	SY	25	$ 13.00	$ 325.00
2.06	Regular Excavation 115'x 15'x12'	CY	767	$ 35.00	$ 26,845.00
2.07	Borrow Excavation, Truck Measure	CY	0	$ 30.00	$ -
2.08	Embankment	CY	0	$ 30.00	$ -
2.09	Excavation for Structures	CY	0	$ 30.00	$ -
				Subtotal-Section 2	**$ 27,170.00**

Pay Item	Descriptions	Unit	Qty	Maximum Unit Price $'s	Extended Price $'s for Task Order
3.00 Water Main Potable/Reclaimed (Including fittings, pipe, materials and restoration)					
3.01	Utility Pipe, F&I, Water Main, 2" PVC DR18	LF	0	$ 25.00	$ -
3.02	Utility Pipe, F&I, Water Main, 4" PVC DR18	LF	0	$ 27.00	$ -

EMAILED 8/26/2024

Attachment: Black Sands Bid (2024-R-83 : 2Nd St and Carswell Ave Depression in Road)

3.03	Utility Pipe, F&I, Water Main, 6" PVC DR18	LF	0	$ 35.00	$ -
3.04	Utility Pipe, F&I, Water Main, 8" PVC DR18	LF	0	$ 44.00	$ -
3.05	Utility Pipe, F&I, Water Main, 10" PVC DR18	LF	0	$ 53.00	$ -
3.06	Utility Pipe, F&I, Water Main, 12" PVC DR18	LF	0	$ 59.00	$ -
3.07	Utility Pipe, F&I, Water Main, 16" PVC DR18	LF	0	$ 63.00	$ -
3.08	Utility Pipe, F&I, Water Main, 18" PVC DR18	LF	0	$ 70.00	$ -
3.09	Utility Pipe, F&I, Water Main, 20" PVC DR18	LF	0	$ 75.00	$ -
3.10	Utility Pipe, F&I, Water Main 2" Directional Drill HDD/HDPE	LF	400	$ 82.81	$ 33,124.00
3.11	Utility Pipe, F&I, Water Main 4" Directional Drill HDD/HDPE	LF	0	$ 100.31	$ -
3.12	Utility Pipe, F&I, Water Main 6" Directional Drill HDD/HDPE	LF	0	$ 115.99	$ -
3.13	Utility Pipe, F&I, Water Main 8" Directional Drill HDD/HDPE	LF	0	$ 133.89	$ -
3.14	Utility Pipe, F&I, Water Main 10" Directional Drill HDD/HDPE	LF	0	$ 158.75	$ -
3.15	Utility Pipe, F&I, Water Main 12" Directional Drill HDD/HDPE	LF	0	$ 195.14	$ -
3.16	Utility Pipe, Water Main, Remove/Dispose, Galv. 0"-1.9"	LF	0	$ 15.00	$ -
3.17	Utility Pipe, Water Main, Remove/Dispose, 2"	LF	0	$ 17.00	$ -
3.18	Utility Pipe, Water Main, Remove/Dispose, 4"	LF	0	$ 18.00	$ -
3.19	Utility Pipe, Water Main, Remove/Dispose, 6"	LF	0	$ 20.00	$ -
3.20	Utility Pipe, Water Main, Remove/Dispose, 8"	LF	0	$ 20.00	$ -
3.21	Utility Pipe, Water Main, Remove/Dispose, 10"	LF	0	$ 22.00	$ -
3.22	Utility Pipe, Water Main, Remove/Dispose, 12"	LF	0	$ 25.00	$ -
3.23	Utility Pipe, Water Main, Plug & Out of Service, 0"-1.9"	LF	0	$ 14.00	$ -
3.24	Utility Pipe, Water Main, Plug & Out of Service, 2"	LF	0	$ 15.00	$ -
3.25	Utility Pipe, Water Main, Plug & Out of Service, 4"	LF	0	$ 16.00	$ -
3.26	Utility Pipe, Water Main, Plug & Out of Service, 6"	LF	0	$ 18.00	$ -
3.27	Utility Pipe, Water Main, Plug & Out of Service, 8"	LF	0	$ 20.00	$ -
3.28	Utility Pipe, Water Main, Plug & Out of Service, 10"	LF	0	$ 20.00	$ -
3.29	Utility Pipe, Water Main, Plug & Out of Service, 12"	LF	0	$ 22.00	$ -
				Subtotal-Section 3	**$ 33,124.00**

Pay Item	Descriptions	Unit	Qty	Maximum Unit Price $'s	Extended Price $'s for Task Order
4.00 Dewatering Equipment not otherwise specified under installation line items					
4.01	Quiet dewatering system (minimum 200 foot with well points for up t	LS	1	$ 10,600.00	$ 10,600.00
4.02	Driveway Crossings (28 Days each)	LS	0	$ 21.00	$ -
4.03	Additional Well Points	EA	0	$ 55.00	$ -
4.04	Additional Header pipe	LF	0	$ 7.75	$ -
4.05	Sand for well per load (up to 400 foot of well points)	EA	0	$ 265.00	$ -
				Subtotal-Section 4	**$ 10,600.00**

Pay Item	Descriptions	Unit	Qty	Maximum Unit Price $'s	Extended Price $'s for Task Order
5.00 Utility - Water Services (Including fittings, pipe, materials and restoration)					
5.01	Utility Fixture, F&I, Water, Meter and Meter Box on 0"-1.9" WM	EA	0	$ 750.00	$ -
5.02	Utility Fixture, F&I, Water, Backflow Assembly on 0"-1.9" WM	EA	0	$ 850.00	$ -
5.03	Utility Fixture, F&I, Water, Saddle on 0"-1.9" WM	EA	0	$ 250.00	$ -
5.04	Utility Fixture, F&I, Water, Gate Valve Assembly on 0"-1.9" WM	EA	0	$ 295.00	$ -

Attachment: Black Sands B?id (2024-R-83 : 2Nd St and Carswell Ave Depression in Road)

5.05	Utility Fixture, F&I, Water, Meter and Meter Box on 2" WM	EA	0	$ 850.00	$ -
5.06	Utility Fixture, F&I, Water, Saddle on 2" WM	EA	0	$ 275.00	$ -
5.07	Utility Fixture, F&I, Water, Gate Valve Assembly on 2" WM	EA	0	$ 365.00	$ -
5.08	Utility Fixture, F&I, Water, Line Stop Assembly on 2" WM	EA	0	$ 4,850.00	$ -
5.09	Utility Fixture, F&I, Water, Mech Joint Restraint on 2" WM	EA	0	$ 125.00	$ -
5.10	Utility Fixture, F&I, Water, Meter and Meter Box on 4" WM	EA	0	$ 825.00	$ -
5.11	Utility Fixture, F&I, Water, Saddle on 4" WM	EA	0	$ 200.00	$ -
5.12	Utility Fixture, F&I, Water, Gate Valve Assembly on 4" WM	EA	0	$ 675.00	$ -
5.13	Utility Fixture, F&I, Water, Line Stop Assembly on 4" WM	EA	0	$ 7,230.00	$ -
5.14	Utility Fixture, F&I, Water, Mech Joint Restraint on 4" WM	EA	0	$ 205.00	$ -
5.15	Utility Fixture, F&I, Water, Meter and Meter Box on 6" WM	EA	0	$ 825.00	$ -
5.16	Utility Fixture, F&I, Water, Saddle on 6" WM	EA	0	$ 850.00	$ -
5.17	Utility Fixture, F&I, Water, Gate Valve Assembly on 6" WM	EA	0	$ 2,250.00	$ -
5.18	Utility Fixture, F&I, Water, Line Stop Assembly on 6" WM	EA	0	$ 8,240.00	$ -
5.19	Utility Fixture, F&I, Water, Mech Joint Restraint on 6" WM	EA	0	$ 250.00	$ -
5.20	Utility Fixture, F&I, Water, Meter and Meter Box on 8" WM	EA	0	$ 925.00	$ -
5.21	Utility Fixture, F&I, Water, Saddle on 8" WM	EA	0	$ 1,005.00	$ -
5.22	Utility Fixture, F&I, Water, Gate Valve Assembly on 8" WM	EA	0	$ 2,400.00	$ -
5.23	Utility Fixture, F&I, Water, Line Stop Assembly on 8" WM	EA	0	$ 9,405.00	$ -
5.24	Utility Fixture, F&I, Water, Mech Joint Restraint on 8" WM	EA	0	$ 375.00	$ -
5.25	Utility Fixture, F&I, Water, Meter and Meter Box on 10" WM	EA	0	$ 925.00	$ -
5.26	Utility Fixture, F&I, Water, Saddle on 10" WM	EA	0	$ 1,150.00	$ -
5.27	Utility Fixture, F&I, Water, Gate Valve Assembly on 10" WM	EA	0	$ 3,250.00	$ -
5.28	Utility Fixture, F&I, Water, Line Stop Assembly on 10" WM	EA	0	$ 10,280.00	$ -
5.29	Utility Fixture, F&I, Water, Mech Joint Restraint on 10" WM	EA	0	$ 525.00	$ -
5.30	Utility Fixture, F&I, Water, Meter and Meter Box on 12" WM	EA	0	$ 1,025.00	$ -
5.31	Utility Fixture, F&I, Water, Saddle on 12" WM	EA	0	$ 1,250.00	$ -
5.32	Utility Fixture, F&I, Water, Gate Valve Assembly on 12" WM	EA	0	$ 3,950.00	$ -
5.33	Utility Fixture, F&I, Water, Line Stop Assembly on 12" WM	EA	0	$ 10,745.00	$ -
5.34	Utility Fixture, F&I, Water, Mech Joint Restraint on 12" WM	EA	0	$ 3,500.00	$ -
5.35	Utility Fixture, F&I, 1" Single Short Water Service on 0"-2"	EA	0	$ 750.00	$ -
5.36	Utility Fixture, F&I, 1" Single Long Water Service on 0"-2"	EA	0	$ 2,000.00	$ -
5.37	Utility Fixture, F&I, 1.5" Double Short Water Service on 0"-2"	EA	0	$ 800.00	$ -
5.38	Utility Fixture, F&I, 1.5" Double Long Water Service on 0"-2"	EA	0	$ 2,200.00	$ -
5.43	Utility Fixture, F&I, 1" Single Short Water Service on 4"	EA	0	$ 775.00	$ -
5.44	Utility Fixture, F&I, 1" Single Long Water Service on 4"	EA	0	$ 2,050.00	$ -
5.45	Utility Fixture, F&I, 1.5" Double Short Water Service on 4"	EA	0	$ 825.00	$ -
5.46	Utility Fixture, F&I, 1.5" Double Long Water Service on 4"	EA	0	$ 2,225.00	$ -
5.47	Utility Fixture, F&I, 1" Single Short Water Service on 6"	EA	0	$ 800.00	$ -
5.48	Utility Fixture, F&I, 1" Single Long Water Service on 6"	EA	0	$ 2,050.00	$ -
5.49	Utility Fixture, F&I, 1.5" Double Short Water Service on 6"	EA	0	$ 850.00	$ -
5.50	Utility Fixture, F&I, 1.5" Double Long Water Service on 6"	EA	0	$ 2,250.00	$ -
5.51	Utility Fixture, F&I, 1" Single Short Water Service on 8"	EA	0	$ 800.00	$ -
5.52	Utility Fixture, F&I, 1" Single Long Water Service on 8"	EA	0	$ 2,100.00	$ -
5.53	Utility Fixture, F&I, 1.5" Double Short Water Service on 8"	EA	0	$ 900.00	$ -
5.54	Utility Fixture, F&I, 1.5" Double Long Water Service on 8"	EA	0	$ 2,300.00	$ -
5.55	Utility Fixture, F&I, 1" Single Short Water Service on 10"	EA	0	$ 950.00	$ -

Attachment: Black Sands B?id (2024-R-83 : 2Nd St and Carswell Ave Depression in Road)

5.56	Utility Fixture, F&I, 1" Single Long Water Service on 10"	EA	0	$ 2,400.00	$ -
5.57	Utility Fixture, F&I, 1.5" Double Short Water Service on 10"	EA	0	$ 1,000.00	$ -
5.58	Utility Fixture, F&I, 1.5" Double Long Water Service on 10"	EA	0	$ 2,600.00	$ -
5.59	Utility Fixture, F&I, 1" Single Short Water Service on 12"	EA	0	$ 1,100.00	$ -
5.60	Utility Fixture, F&I, 1" Single Long Water Service on 12"	EA	0	$ 2,500.00	$ -
5.61	Utility Fixture, F&I, 1.5" Double Short Water Service on 12"	EA	0	$ 1,200.00	$ -
5.62	Utility Fixture, F&I, 1.5" Double Long Water Service on 12"	EA	0	$ 2,600.00	$ -
5.63	Utility Fixture, F&I, Single Meter Box	EA	0	$ 350.00	$ -
5.64	Utility Fixture, F&I, Double Meter Box	EA	0	$ 500.00	$ -
				Subtotal-Section 5	**0**

Pay Item	Descriptions	Unit	Qty	Maximum Unit Price $'s	Extended Price $'s for Task Order
6.00	**Fire Hydrants**				
6.01	Fire Hydrant Assembly, Stnd 3 Way, F&I, 6"	EA	0	$ 7,800.00	$ -
6.02	Fire Hydrant, Adjust & Modify	EA	0	$ 3,700.00	$ -
6.03	Fire Hydrant Relocate	EA	0	$ 3,700.00	$ -
6.04	Fire Hydrant Remove	EA	0	$ 2,600.00	$ -
6.05	FH Assembly Connection Fitting - 6"x6"x6" MJ Tee - FH to Main	EA	0	$ 1,030.00	$ -
6.06	FH Assembly Connection Fitting - 8"x8"x6" MJ Tee - FH to Main	EA	0	$ 1,270.00	$ -
6.07	FH Assembly Connection Fitting-10"x10"x6" MJ Tee-FH to	EA	0	$ 1,790.00	$ -
6.08	FH Assembly Connection Fitting-12"x12"x6" MJ Tee-FH to	EA	0	$ 2,037.50	$ -
6.09	FH Assembly Connection Fitting - 6" MJ 90° Elbow - FH to	EA	0	$ 695.00	$ -
6.10	FH Assembly Connection Fitting - 8" MJ 90° Elbow - FH to	EA	0	$ 970.00	$ -
6.11	FH Assembly Connection Fitting-10" MJ 90° Elbow - FH to	EA	0	$ 1,607.50	$ -
6.12	FH Assembly Connection Fitting-12" MJ 90° Elbow - FH to	EA	0	$ 1,917.50	$ -
				Subtotal-Section 6	**$ -**

Pay Item	Descriptions	Unit	Qty	Maximum Unit Price $'s	Extended Price $'s for Task Order
7.00	**Utility - Sewer Service (Including fittings, pipe, materials and restoration)**				
7.01	Utility Pipe, F&I, Sewer, 2" PVC DR18	LF	0	$ 200.00	$ -
7.02	Utility Pipe, F&I, Sewer, 4" PVC DR18	LF	0	$ 220.00	$ -
7.03	Utility Pipe, F&I, Sewer, 6" PVC DR18	LF	0	$ 230.00	$ -
7.04	Utility Pipe, F&I, Sewer, 8" PVC DR18	LF	115	$ 235.00	$ 27,025.00
7.05	Utility Pipe, F&I, Sewer, 10" PVC DR18	LF	0	$ 240.00	$ -
7.06	Utility Pipe, F&I, Sewer, 12" PVC DR18	LF	0	$ 260.00	$ -
7.07	Utility Pipe, Sewer, Remove/Dispose, 4"	LF	0	$ 20.00	$ -
7.08	Utility Pipe, Sewer, Remove/Dispose, 6"	LF	0	$ 22.00	$ -
7.09	Utility Pipe, Sewer, Remove/Dispose, 8"	LF	0	$ 24.00	$ -
7.10	Utility Pipe, Sewer, Remove/Dispose, 10"	LF	0	$ 28.00	$ -
7.11	Utility Pipe, Sewer, Remove/Dispose, 12"	LF	0	$ 28.00	$ -
7.12	Utility Fixture, F&I, 6" Single Short Sewer Service on 6"	EA	0	$ 2,400.00	$ -
7.13	Utility Fixture, F&I, 6" Single Long Sewer Service on 6"	EA	0	$ 6,800.00	$ -
7.14	Utility Fixture, F&I, 6" Single Short Sewer Service on 8"	EA	0	$ 2,500.00	$ -
7.15	Utility Fixture, F&I, 6" Single Long Sewer Service on 8"	EA	0	$ 7,000.00	$ -

Attachment: Black Sands B?id (2024-R-83 : 2Nd St and Carswell Ave Depression in Road)

7.16	Utility Fixture, F&I, 6" Single Short Sewer Service on 10"	EA	0	$ 2,850.00	$ -
7.17	Utility Fixture, F&I, 6" Single Long Sewer Service on 10"	EA	0	$ 7,200.00	$ -
7.18	Utility Fixture, F&I, 6" Single Short Sewer Service on 12"	EA	0	$ 2,950.00	$ -
7.19	Utility Fixture, F&I, 6" Single Long Sewer Service on 12"	EA	0	$ 7,500.00	$ -
7.20	Utility Fixture, F&I, 6" Cleanout Sewer on 6"	EA	0	$ 720.00	$ -
7.21	Utility Fixture, F&I, 6" Cleanout Sewer on 8"	EA	0	$ 780.00	$ -
7.22	Utility Fixture, F&I, 6" Cleanout Sewer on 10"	EA	0	$ 850.00	$ -
7.23	Utility Fixture, F&I, 6" Cleanout Sewer on 12"	EA	0	$ 925.00	$ -
7.24	Sewer Manhole Complete Depth 0 to 8 foot	EA	0	$ 8,900.00	$ -
7.25	Sewer Manhole Complete Depth 8.1 to16 foot	EA	0	$ 12,600.00	$ -
7.26	Sewer Manhole Complete Depth 16.1 to 24 foot	EA	0	$ 14,900.00	$ -
7.27	Connect to Sewer Manhole	EA	0	$ 3,100.00	$ -
				Subtotal-Section 7	**$ 27,025.00**

Pay Item	Descriptions	Unit	Qty	Maximum Unit Price $'s	Extended Price $'s for Task Order
8.00	**Supplemental and Emergency Services (Hourly labor rates with appropriate equipment and tools for response as needed)**				
8.01	Mobilization for supplemental and emergency response	LS	0	$ 2,400.00	$ -
8.02	Crew Regular (Minimum 4 HRs)	HR	0	$ 444.47	$ -
8.03	Crew After-Hr Response Typically 5PM to 6AM (Min. 4 HRs)	HR	0	$ 544.52	$ -
8.04	Dump Truck with Operator (Min. 4 HRs)	HR	0	$ 484.00	$ -
8.05	Additional Labor (Min. 4 HRs)	HR	0	$ 385.00	$ -
				Subtotal-Section 8	**$ -**

Pay Item	Descriptions	Unit	Qty	Maximum Unit Price $'s	Extended Price $'s for Task Order
9.00	**Concrete and Temporary Road Plat Services.**				
9.01	Sidewalk Concrete, 4" thick	SY	0	$ 54.00	$ -
9.02	Sidewalk Concrete, 6" thick	SY	0	$ 72.00	$ -
9.03	Driveway Apron Concrete, 6" thick	SY	0	$ 80.00	$ -
9.04	Steel Vehicular Plates, Temp., F&I 8' W x 10' L x 1" thick	EA	0	$ 2,199.50	$ -
				Subtotal-Section 10	**$ -**

Pay Item	Descriptions	Unit	Qty	Maximum Unit Price $'s	Extended Price $'s for Task Order
10.00	**Roadway and Right of Way Subbase Restoration**				
10.01	Stabilization Fill (FDOT Standard)	SY	0	$ 18.00	$ -
10.02	Optional Base Group 06 or 8" Lime rock (FDOT Standard)	SY	0	$ 54.00	$ -
10.03	Temporary Asphalt Parching (cold or hot patch up to 2" thick)	SY	0	$ 89.00	$ -
				Subtotal-Section11	**$ -**

Pay Item	Descriptions	Unit	Qty	Maximum Unit Price $'s	Extended Price $'s for Task Order

Attachment: Black Sands B?id (2024-R-83 : 2Nd St and Carswell Ave Depression in Road)

11.00 Stormwater Improvements and Restoration					
11.01	Curb Inlet Complete, F&I-TypeP, 4'Dia Rnd, Type1 Top, 6' OAH	EA	0	$ 7,995.11	$ -
11.02	Curb Inlet Complete, F&I-TypeP, 4'Dia Rnd, Type2 Top, 6' OAH	EA	0	$ 8,268.93	$ -
11.03	Curb Inlet Complete, F&I-TypeJ, 5'Dia Rnd, Type1 Top, 6' OAH	EA	0	$ 9,694.29	$ -
11.04	Curb Inlet Complete, F&I-Type J, 5' Dia Rnd, Type2 Top, 6'	EA	0	$ 10,151.93	$ -
11.05	Curb Inlet Complete, F&I-TypeP, 4' Dia Rnd, Type5 Top, 6'	EA	0	$ 7,167.14	$ -
11.06	Curb Inlet Complete, F&I-TypeP, 4' Dia Rnd, Type6 Top, 6'	EA	0	$ 8,013.12	$ -
11.07	Curb Inlet Complete, F&I-TypeJ, 5' Dia Rnd, Type5 Top, 6'	EA	0	$ 9,276.38	$ -
11.08	Curb Inlet Complete, F&I-TypeJ, 5' Dia Rnd, Type6 Top, 6'	EA	0	$ 9,896.62	$ -
11.09	Ditch Bottom Inlet, F&I -Type C, 3' Square, 6' OAH	EA	0	$ 6,463.38	$ -
11.10	Ditch Bottom Inlet, F&I -Type D, 5' Square, 6' OAH	EA	0	$ 9,536.68	$ -
11.11	Ditch Bottom Inlet, F&I -Type E, 4' Square, 6' OAH	EA	0	$ 8,459.07	$ -
11.12	Ditch Bottom Inlet, F&I -Type H, 4 x 7 Rectangle, 6' OAH	EA	0	$ 11,296.33	$ -
11.13	USF 5100 Valley Gutter Inlet Frame and 6147 Grate or Equiv.	EA	0	$ 2,694.00	$ -
11.14	Manhole Complete, F&I-TypeP, 4' Dia. Rnd, Type8 Top, 6'	EA	0	$ 7,284.82	$ -
11.15	Manhole Adjust to Grade Existing	EA	0	$ 2,850.00	$ -
11.16	Pipe Culvert, F&I, RCP, Round, 15"	LF	0	$ 94.00	$ -
11.17	Pipe Culvert, F&I, RCP, Round, 18"	LF	0	$ 117.00	$ -
11.18	Pipe Culvert, F&I, RCP, Round, 24"	LF	0	$ 135.00	$ -
11.19	Pipe Culvert, F&I, RCP, Round, 30"	LF	0	$ 165.00	$ -
11.20	Pipe Culvert, F&I, RCP, Round, 36"	LF	0	$ 202.00	$ -
11.21	Pipe Culvert, F&I, RCP, Round, 42"	LF	0	$ 259.00	$ -
11.22	Pipe Culvert, F&I, RCP, Round, 48"	LF	0	$ 311.00	$ -
11.23	Pipe Culvert, F&I, RCP, Round, 54"	LF	0	$ 383.00	$ -
11.24	Pipe Culvert, F&I, RCP, Round, 60"	LF	0	$ 465.00	$ -
11.25	Pipe Culvert, F&I, ERCP, Round, 12 x 18" (15")	LF	0	$ 89.00	$ -
11.26	Pipe Culvert, F&I, ERCP, Round, 14 x 23" (18")	LF	0	$ 124.00	$ -
11.27	Pipe Culvert, F&I, ERCP, Round, 19 x 30" (24")	LF	0	$ 169.00	$ -
11.28	Pipe Culvert, F&I, ERCP, Round, 24 x 38" (30")	LF	0	$ 205.00	$ -
11.29	Pipe Culvert, F&I, ERCP, Round, 29 x 45" (36")	LF	0	$ 272.00	$ -
11.30	Pipe Culvert, F&I, ERCP, Round, 34 x 53" (42")	LF	0	$ 352.00	$ -
11.31	Pipe Culvert, F&I, ERCP, Round, 38 x 60" (48")	LF	0	$ 426.00	$ -
11.32	Pipe Culvert, F&I, ERCP, Round, 43 x 68" (54")	LF	0	$ 533.50	$ -
11.33	Pipe Culvert, F&I, HDPE, Round, 12"	LF	0	$ 35.30	$ -
11.34	Pipe Culvert, F&I, HDPE, Round, 15"	LF	0	$ 45.69	$ -
11.35	Pipe Culvert, F&I, HDPE, Round, 18"	LF	0	$ 57.13	$ -
11.34	Pipe Culvert, F&I, HDPE, Round, 24"	LF	0	$ 83.35	$ -
11.35	Pipe Culvert, F&I, HDPE, Round, 30"	LF	0	$ 110.73	$ -
11.36	Pipe Culvert, F&I, HDPE, Round, 36"	LF	0	$ 138.00	$ -
11.37	Mitered End Section Complete, F&I, RCP, Round, 15" Pipe	EA	0	$ 1,500.00	$ -
11.38	Mitered End Section Complete, F&I, RCP, Round, 18" Pipe	EA	0	$ 1,800.00	$ -
11.39	Mitered End Section Complete, F&I, RCP, Round, 24" Pipe	EA	0	$ 2,400.00	$ -
11.40	Mitered End Section Complete, F&I, RCP, Round, 30" Pipe	EA	0	$ 2,900.00	$ -
				Subtotal-Section 12	**$ -**

Pay Item	Descriptions	Unit	Qty	Maximum Unit Price $'s	Extended Price $'s for Task Order

Attachment: Black Sands B?id (2024-R-83 : 2Nd St and Carswell Ave Depression in Road)

12.00 Landscape Restoration					
12.01	Turf Sod (installation and rolling of Bahia or St. Augustine)	SY	0	$ 6.25	$ -
12.01	Irrigation System Repairs	EA	0	$ 225.00	$ -
				Subtotal-Section 13	**$ -**

Pay Item	Descriptions	Unit	Qty	Maximum Unit Price $'s	Extended Price $'s for Task Order
13.00	**Out-of-Scope Items**				
13.01	Out of Scope Item(s) includes receiving, installation and tax. The Contractor shall receive quotes for all out of scope items. Out of scope items may not exceed 10% markup. The City reserves option to owner direct purchase materials under ODP guidelines. **(The total Out of Scope item(s) may not exceed 49% of Total Work Order Assignment)**	LS	No Bid Item	TBA 10 % maximum markup from List below.	2496
	Out of Scope Item Descripton = Asphalt Removal	SY	192	13	2496
	Out of Scope Item Descripton =			0	0
	Out of Scope Item Descripton =			0	0
	Out of Scope Item Descripton =			0	0
	TOTAL EXTENDED PRICE OF ALL LINE ITEMS 1.00 to 12.00 (Base Quantity = 1 for bid evaluation only)	$			**$ 97,919.00**

Unit Price and Quatity will be issued to determine future project and restoration services cost, as requested.

1.01	Mobilization/Demobilization (Not exceed 10% of task order)	%	0.10	10%	$ 9,791.90
1.02	Maintenance of Traffic (Not to exceed 5% of task order)	%	0.00	5%	$ -
1.09	FL/Federal Funding Req. (Not exceed 5% of task order)	%	0.05	5%	

Total (% make-ups for 1.01. 102,& 1.09) **$ 107,710.90**

TOTAL T.O. $ 110,206.90

Attachment: Black Sands B?id (2024-R-83 : 2Nd St and Carswell Ave Depression in Road)



Attachment: 2nd Street at

HOLLY HILL
FLORIDA

STAFF REPORT
CITY OF HOLLY HILL, FLORIDA

City Commission
Resolution

MEETING DATE: October 22, 2024
FROM: Antoine Khoury
SUBJECT: A Resolution of the City of Holly Hill, Florida, Approving the Piggyback of Charlotte County Contract #2021000541, Awarding the Purchase of (4) 2024 Police Vehicles from Bartow Ford at a Cost of $211,144.11 and Authorizing the City Manager to Execute the Same; Providing for Severability; and Providing for an Effective Date.
NUMBER: 2024-R-84
APPLICANT:
PLANNER:

DISCUSSION:

In keeping with the City's fleet replacement plan, two (2) Police Interceptors, and one (1) Police Ford Explorer have been approved to purchase in the fiscal year 2024/2025 budget. Also approved is one (1) F150 for the Fire Department in the fiscal year 2024/2025 budget. This Resolution authorizes the City Manager to utilize a piggyback agreement between Charlotte County and Bartow Ford for the purchase of police rated vehicles. This contract offers a 4.27% discount off of Ford Factory Invoices and a 0% mark-up on dealer installed options.

Charlotte County contract # 2021000541 was awarded on September 14, 2021 and has been extended through December 31, 2024. Charlotte County contract # 2021000541 is included under "Exhibit A".

Items requested to be purchased this year include:

One (1) 2024 Ford Interceptor Utility K9 vehicle at a cost of $60,444.17.

One (1) 2024 Ford Interceptor Utility vehicle at a cost of $56,316.17.

One (1) 2024 Ford Explorer Captain's vehicle at a cost of $39,814.50.

One (1) 2023 F-150 Police Responder Pick-Up truck at a cost of $54,569.27.

The total cost of police vehicles to be purchased through this resolution is $211,144,11.

Proposals from Bartow Ford including unit pricing of vehicles are included under "Exhibits B, C, D and E".

Current City of Holly Hill Purchasing Manual

Policy 2.39 Other Government Entities' Contracts.

The City may utilize (piggy-back) any other government entity's open contract that have been competitively bid and awarded to the low responsive, responsible bidder meeting the specifications, in accordance with City Purchasing regulations. The City may also piggyback off U.S. General Services Administration, GSA Contracts. When another entity's contracts is the be utilized, a copy of that contract shall be forwarded to the Finance Department for review and evaluation to determine if it meets the City's requirement regarding competitive bidding and award.

Chapter 287, Florida Statutes, grants the authority to piggyback the purchase of goods and services as a form of intergovernmental cooperative purchasing in which a public purchaser requests competitive sealed bids, enters into a contract, and arranges, as part of the contract, for other public purchasing units to purchase from the selected vendor under the same terms and conditions as itself in order to take advantage of the better pricing that large purchasers are able to obtain in order to reduce administrative time and costs involved in the procurement process (i.e., cost of preparing bid specifications, advertising, etc.).

Section 2.39 of the City's Purchasing Policy is included under "Exhibit C".

FISCAL ANALYSIS:

Capital projects for the purchase of (3) Police vehicles and (1) Fire vehicle were adopted in the fiscal year 2024/2025 budget in general ledger account 001-8110-580-6400 at an anticipated cost of $211,144.11. These capital purchases are represented by Project Codes 25FD01, 25PD01, 25PD02 and 25PD03 respectively.

STAFF RECOMMENDATION:

That the City Commission approve the piggyback of Charlotte County contract # 2021000541 with Bartow Ford, award the purchase of (3) 2024 Police vehicles and (1) Fire vehicle from Bartow Ford at a cost of $211,144.11 and authorize the City Manager to execute the same.

COMMISSION GOAL:

Goal #1: Develop and maintain a sound and sustainable financial plan for the city that establishes sufficient reserves for all funds, ensures (whenever possible) that user fees pay for services rendered, provides a realistic capital improvement program, and encourages public/private sector partnerships and intergovernmental partnerships.

Goal #2: Enhance City aesthetics through beautification and maintenance of city property and public rights of way, consistent enforcement of zoning and property maintenance codes, and development of reasonable design standards and a corresponding process which is applicable to all new developments and business improvements in the city.

MOTION:

APPROVING THE PIGGY-BACK OF CHARLOTTE COUNTY CONTRACT # 2021000541, AWARDING THE PURCHASE OF (3) 2024 POLICE VEHICLES AND (1) FIRE VEHICLE FROM BARTOW FORD AT A COST OF $211,144.11 AND AUTHORIZING THE CITY MANAGER TO EXECUTE THE SAME.

ATTACHMENTS:

- Exhibit A - Charlotte Co Contract 2021000541 (PDF)
- Exhibit B - Bartow Ford Interceptor $60k (PDF)
- Exhibit C - Bartow Ford Police Interceptor (PDF)
- Exhibit D - Bartow Ford Explorer (PDF)
- Exhibit E - Bartow Ford FD F150 (PDF)

Resolution No. 2024-84

A RESOLUTION OF THE CITY OF HOLLY HILL, FLORIDA, APPROVING THE PIGGYBACK OF CHARLOTTE COUNTY CONTRACT #2021000541, AWARDING THE PURCHASE OF (4) 2024 POLICE VEHICLES FROM BARTOW FORD AT A COST OF $211,144.11 AND AUTHORIZING THE CITY MANAGER TO EXECUTE THE SAME; PROVIDING FOR SEVERABILITY; AND PROVIDING FOR AN EFFECTIVE DATE.

A RESOLUTION OF THE CITY OF HOLLY HILL, FLORIDA, APPROVING THE PIGGYBACK OF CHARLOTTE COUNTY CONTRACT #2021000541, AWARDING THE PURCHASE OF (4) 2024 POLICE VEHICLES FROM BARTOW FORD AT A COST OF $211,144.11 AND AUTHORIZING THE CITY MANAGER TO EXECUTE THE SAME; PROVIDING FOR SEVERABILITY; AND PROVIDING FOR AN EFFECTIVE DATE.

WHEREAS, two Police Interceptors, one Police Explorer, and one Police F-150 vehicles were approved to be purchased in the adopted fiscal year 2024-2025 budget in keeping with the Fleet vehicle replacement plan; and

WHEREAS, the City of Holly Hill desires to purchase the vehicles under Charlotte County Vehicle Purchase contract #2021000541, under the same terms and applicable conditions as that agreement; and

WHEREAS, Chapter 287, Florida Statutes, grants the authority to piggyback the purchase of goods and services as a form inter-governmental cooperative purchasing in which a public purchaser requests competitive sealed bids, enters into a contract, and arranges, as part of the contract, for other public purchasing units to purchase from the selected vendor under the same terms and conditions as itself in order to take advantage of the better pricing that large purchasers are able to obtain in order to reduce administrative time and costs involved in the procurement process (i.e., cost of preparing bid specifications, advertising, etc.); and

WHEREAS, pursuant to the City's purchasing policy, "piggyback" contracts are allowed for existing government contracts; and

WHEREAS, the City Commission of the City now desires to authorize and approve the form of the contract by Charlotte County and any other related documents; and

WHEREAS, the City has determined that in this circumstance, piggybacking onto an agreement entered into by the Charlotte County, is the most economically advantageous way to procure these goods and services; and

NOW, THEREFORE, BE IT RESOLVED BY THE CITY COMMISSION

OF THE CITY OF HOLLY HILL, FLORIDA:

SECTION 1. Pursuant to the City's purchasing policy, "piggyback" contracts are allowed for existing government contracts.

SECTION 2. It is hereby ascertained, determined and declared that it is in the best interest of the City to enter into a contract with Bartow Ford for the purchase of Police Interceptor vehicles and equipment.

SECTION 3. SEVERABILITY. If any section or portion of a section of this Resolution proves to be invalid, unlawful, or unconstitutional, it shall not be held to invalidate or impair the validity, force, or effect of any other section or part of this Resolution.

SECTION 4. EFFECTIVE DATE. This Resolution shall take effect immediately upon its adoption.

APPROVED AND AUTHENTICATED on this 22th day of OCTOBER 2024.

Charlotte County Purchasing Division
Administrative Approval

1. Department Making Request/Name/Extension	2.Date
Fleet Management/True, Alisa/X1549	9/19/2024

3. Requested Motion/Action:

Request the County Administrator approve Change Order #1 to Contract #21-541, Vehicles - Annual Contract, with Bartow Ford, to extend validity date of this contract through and including December 31, 2024 at the same prices, terms, and conditions.

4. Is Item Budgeted?	N/A	**If No, state action required**	
Budget Action:	No action needed. Parts and expenses will be funded by the Fleet Management Fund, and then will be charged back to the department as budgeted in the FY2025 budget process.		
Financial Impact Summary Statement:			
No additional impact.			
Detailed Analysis Attached?	N/A	**Reviewed By:**	Daniels, Harold, Senior Financial Analyst- 09/19/2024

5. Background (Why is the action necessary and what action will be accomplished)

This contract is for the purchase of vehicles on an as needed basis for Charlotte County. The current contract expires on September 30, 2024 and there are no renewal options left. Bartow Ford has been contacted and agreed to extend their current contract wtih Charlotte County to give us time to solicit and establish a new contract.

Therefore, it is requested that the County Administrator approve Change Order #1 to Contract #21-541, Vehicles - Annual Contract, with Bartow Ford, to extend validity date of this contract through and including December 31, 2024 at the same prices, terms, and conditions.

6. Recommended Approvals

Gutierrez, Lorrie, Fleet Operations Manager - 9/24/2024	Corbett, Kimberly, Senior Division Mgr-Purchasing - 9/24/2024	Flores, Hector, County Administrator - 9/24/2024
Department/Division	Purchasing Division	Administration (when applicable)

Attachment: Exhibit A - Charlotte Co Contract 2021000541 (2024-R-84 : Purchase of New Police & Fire Department Vehicles)

Charlotte County Government

"To exceed expectations in the delivery of public services."

www.CharlotteCountyFL.gov

9/19/2024

Richard Weissinger, Commercial Fleet Sales
BARTOW FORD
2800 US Hwy 98 North
Bartow, FL 33830

Dear Mr. Weissinger:

With reference to our Bid No. 2021000541, Vehicles – Annual Contract, Charlotte County would like to request your approval to extend the validity date of this contract through and including December 31, 2024, at the same prices, terms, and conditions.

Please respond at your earliest possible convenience, as your signed approval is required in order to acknowledge this extension. If you have any questions, please contact Alisa L. True, CPPB, Senior Contract Specialist, at 941-743-1549.

Yours truly,

Alisa True for
Kimberly A. Corbett, C.P.M., CPPB
Senior Division Manager - Purchasing

KAC/at

☒ Yes, I am interested in extending the validity of my contract with Charlotte County through and including December 31, 2024, under the same prices, terms, and conditions of the original contract.

☐ No thank you, I am not interested in extending the validity of my contract with Charlotte County.

Richard Weissinger 9/19/24
Richard Weissinger date

cc: File

PURCHASING
18500 Murdock Circle, Suite 344 | Port Charlotte, FL 33948
Phone: 941.743.1374 | Fax: 941.743.1384

Attachment: Exhibit A - Charlotte Co Contract 2021000541 (2024-R-84 : Purchase of New Police & Fire Department Vehicles)

BARTOW FORD
INTEGRITY•TRUST•HONESTY
Since 1948

July 23, 2024

City of Holly Hill
SGT. Weiss

	DESCRIPTION	
K8A	2024 Police Interceptor Utility AWD	
99B	3.3L V6 Direct-Injection (FFV) V-6 Engine	
44U	10 Speed Automatic Transmission	
86T	Rear Taillight Prep Package Pre-existing holes with standard twist lock sealed capability (does not include LED installed lights) eliminates need to drill housing assemblies	
43D	Dark Car Feature	
60A	Factory Grill, Lamp, Siren & Speaker Wiring	
51T	Factory Pillar Mounted LED Spotlight	
65L	18" 5-Spoke Full Face Wheel Covers w/Metal Clips	
55F	Remote Keyless Entry Key Fob	
76R	Reverse Sensing	
	Rear View Camera	
76P	Pre-Collision Assist w/Pedestrian Detection	
52T	Class III Trailer Tow Lighting Package Includes 4-pin and 7-pin connectors and wiring.	
17A	Rear Air Conditioning	
	Factory Invoice	$46,549.00
	Government Price Concession Discount	$1,800.00
	4.27% Contract Discount	$1,910.78
	Whelen DUO FST Red/Blue Inneredge Lightbar with White Takedown, Whelen CORE Siren Controller, (1) 100 Watt Speaker, (1) Whelen Red MICRON Mounted in Grill Area, (1) Whelen Blue MICRON Mounted in Grill Area, (1) Whelen Spitfire DUO ION Red/Blue ION Mounted in Lower Windshield Area, Inner Edge RST DUO Rear Facing Bar 10 Head Red/Blue with Amber Traffic Advisor Mounted inside Rear Hatch Area, (2) Clear LED's Mounted in Headlights & (2) Mounted in Taillights, Wig Wag Headlight Flasher, Flash Taillights, (1) Whelen Red Thin ION Mounted in Tag Area, (1) Whelen Blue Thin ION Mounted in Tag Area, 2 Whelen SOLO 5 Module Tracers R/B/R/B/R, Havis C-VS-1012-INUT-2 Angled Console with Dual Cup Holder & C-ARM-103 Arm Rest, C-OHC-INUT-1 Overhead Console for CORE Siren Controller, 11" Slide Out Locking Swing Arm with Motion Adapter with Docking Station For Getac S410 Notebook With Power Supply Mounting Bracket & Screen Support, Black K9 Prisoner Transport System, 10" Fan with Window Guard, K9 Hot-N-Pop PRO Temperature Alarm & Door Opening System Includes Horn Activation, Siren Activation, Light Activation, Dual Window Drop and One Door Pop Remote with Holster, Water Bowl (SHIPPS LOOSE), Universal Single Weapon Mounted Overhead on K9 Platform, Dual Raised Rear Weapons Vault, K9 Deep Window Tint, Holly Hill POLICE Graphics, Bartow Ford Custom Installation.	$17,467.00
	Yellow CITY Tag	$138.95
		$0.00
	TOTAL PURCHASE AMOUNT PER UNIT	**$60,444.17**

Pricing in accordance with the Charlotte County contract # 2021000541

If you have any questions or need any additional information please feel free contact me anytime.

001-8110-580-6400

25PD03

K9

Sincerely Yours,
Richard Weissinger
Commercial Fleet Sales
Direct Line (813) 477-0052
Fax (863) 533-8485

2800 US Hwy North
Bartow, Florida 33830

Attachment: Exhibit B - Bartow Ford Interceptor $60k (2024-R-84 : Purchase of New Police & Fire Department Vehicles)

BARTOW FORD
INTEGRITY•TRUST•HONESTY
Since 1948

July 23, 2024

City of Holly Hill
SGT. Weiss

	DESCRIPTION	
K8A	2024 Police Interceptor Utility AWD	
99B	3.3L V6 Direct-Injection (FFV) V-6 Engine	
44U	10 Speed Automatic Transmission	
86T	Rear Taillight Prep Package Pre-existing holes with standard twist lock sealed capability (does not include LED installed lights) eliminates need to drill housing assemblies	
43D	Dark Car Feature	
60A	Factory Grill, Lamp, Siren & Speaker Wiring	
51T	Factory Pillar Mounted LED Spotlight	
65L	18" 5-Spoke Full Face Wheel Covers w/Metal Clips	
55F	Remote Keyless Entry Key Fob	
76R	Reverse Sensing	
	Rear View Camera	
76P	Pre-Collision Assist w/Pedestrian Detection	
52T	Class III Trailer Tow Lighting Package Includes 4-pin and 7-pin connectors and wiring.	
17A	Rear Air Conditioning	
	Factory Invoice	$46,549.00
	Government Price Concession Discount	$1,800.00
	4.27% Contract Discount	$1,910.78
	Whelen 55" Legacy Lightbar with FULL LED Takedown Lights WITH Amber Rear Traffic Advisor, Whelen CORE Siren Controller, (1) 100 Watt Speaker, (1) Whelen Red MICRON Mounted in Grill Area, (1) Whelen Blue MICRON Mounted in Grill Area, (1) Whelen DUO ION Spitfire Red/Blue Mounted in Lower Windshield Area, Inner Edge RST DUO Rear Facing Bar 10 Head Red/Blue with Amber Traffic Advisor Mounted inside Rear Hatch Area, (2) Clear LED's Mounted in Headlights & (2) Mounted in Taillights, Wig Wag Headlight Flasher, Flash Taillights, (1) Whelen Red Thin ION Mounted in Tag Area, (1) Whelen Blue Thin ION Mounted in Tag Area, 2 Whelen SOLO 5 Module Tracers R/B/R/B/R, Havis C-VS-1012-INUT-2 Angled Console with Dual Cup Holder & C-ARM-103 Arm Rest, C-OHC-INUT-1 Overhead Console for CORE Siren Controller, 11" Slide Out Locking Swing Arm with Motion Adapter, Docking Station For Getac S410 Notebook With Power Supply Mounting Bracket & Screen Support, 50/50 Wire Mesh & Poly Window Cage Front Partition, Rear Window Bars, Molded Rear Prisoner Seat with Outboard Buckling Seat Belts Intergraded Mesh Rear Cargo Barrier, Universal Dual Weapons Mounted in Recess Area of Partition, Raised Rear Weapons Vault, Holly Hill POLICE Graphics, Bartow Ford Custom Installation.	$13,339.00
	Yellow CITY Tag	$138.95
		$0.00
	TOTAL PURCHASE AMOUNT PER UNIT	**$56,316.17**

Pricing in accordance with the Charlotte County contract # 2021000541

If you have any questions or need any additional information please feel free contact me anytime.

001-8110-580-6400
25PD02
PATROL

Sincerely Yours,
Richard Weissinger
Commercial Fleet Sales
Direct Line (813) 477-0052
Fax (863) 533-8485

2800 US Hwy North
Bartow, Florida 33830

Attachment: Exhibit C - Bartow Ford Police Interceptor (2024-R-84 : Purchase of New Police & Fire Department Vehicles)

BARTOW FORD
INTEGRITY•TRUST•HONESTY
Since 1948

July 27, 2024

City of Holly Hill
SGT. Weiss

	DESCRIPTION	
K7B	2024 Explorer 4dr 4x2	
99H	2.3L EcoBoost I-4 Engine	
44T	10 Speed Automatic Transmission	
52T	Class IV Trailer Tow Package	
	Factory Invoice	$37,861.00
	Government Price Concession Discount	$2,744.00
	4.27% Contract Discount	$1,499.50
	Whelen DUO FST Red/Blue Inneredge Lightbar with White Takedown, Whelen Hand Held CORE Siren Controller, (1) 100 Watt Speaker, (1) Whelen DUO Red/White ION Mounted in Grill Area, (1) Whelen DUO Blue/White ION Mounted in Grill Area, (1) Whelen Spitfire DUO ION Red/Blue ION Mounted in Lower Windshield Area, (1) Whelen DUO ION Spitfire Red/Blue Mounted in Lower Windshield Area, Inner Edge RST DUO Rear Facing Bar 10 Head Red/Blue with Amber Traffic Advisor Mounted inside Rear Hatch Area, (1) Whelen DUO Striplite + Red/Blue Mounted in P/S Rear 1/4 Glass, (1) Whelen DUO Striplite+ Red/ Blue Mounted in D/S Rear 1/4 Glass, (2) Whelen SOLO 5 Module Tracers R/B/R/B/R, Bartow Ford Custom Installation.	$6,197.00
	TOTAL PURCHASE AMOUNT PER UNIT	**$39,814.50**

Pricing in accordance with the Charlotte County contract # 2021000541

If you have any questions or need any additional information please feel free contact me anytime.

Sincerely Yours,
Richard Weissinger
Commercial Fleet Sales
Direct Line (813) 477-0052
Fax (863) 533-8485

001-8110-580-6400
25PD01

ADMIN

Attachment: Exhibit D - Bartow Ford Explorer (2024-R-84 : Purchase of New Police & Fire Department Vehicles)

BARTOW FORD
INTEGRITY•TRUST•HONESTY
Since 1948

August 1, 2024

City of Holly Hill
Chief Bland

	DESCRIPTION	
W1P	2023 F-150 Police Responder 4x4 5.5' box 145" WB XL	
998	3.5L V6 EcoBoost Engine	
44G	10 Speed Automatic Transmission	
64H	18" Aluminum Wheels	
17C	Chrome Front & Rear Bumpers	
595	Fog Lamps	
67T	Integrated Trailer Brake Controller	
67P	Remote Keyless-Entry	
	Factory Invoice	$50,065.00
	Government Price Concession Discount	$3,000.00
	4.27% Contract Discount	$2,009.68
	Whelen FST Inneredge Red/Red with FULL WHITE LED Takedown, Rear WCX Inneredge Red/Red WITH Amber Rear Traffic Advisor, Whelen CORE Siren Controller, (1) 100 Watt Speaker, (4) Whelen Red/White DUO ION's Mounted in Grill Area, (2) Red/White Vertex Mounted in Taillight, Wig Wag Headlight Flasher, (4) Whelen Red/White Thin DUO ION's Mounted in Lower Tailgate Area, 2 Whelen SOLO 5 Module Tracers R/R/R/R/R, 24" Wide Flat Console With 12" Accessory Pocket W/Hinged Lid & Lock, 4.5" Deep, Dual Cup Holder & C-ARM-1001 Arm Rest, 11" Slide Out Locking Swing Arm with Motion Adapter with UT-2007 iPad Mount & Lock, 6" Steel Running Boards, Spray in Bedliner, Deep Window Tint, Bartow Ford Custom Installation.	$9,375.00
	Yellow CITY Tag	$138.95
		$0.00
	TOTAL PURCHASE AMOUNT PER UNIT	**$54,569.27**

Pricing in accordance with the Charlotte County contract # 2021000541

If you have any questions or need any additional information please feel free contact me anytime.

Sincerely Yours,
Richard Weissinger
Commercial Fleet Sales
Direct Line (813) 477-0052
Fax (863) 533-8485

001-B11D-580-6400
25FD01

Attachment: Exhibit E - Bartow Ford FD F150 (2024-R-84 : Purchase of New Police & Fire Department Vehicles)

HOLLY HILL
FLORIDA

STAFF REPORT
CITY OF HOLLY HILL, FLORIDA

City Commission
Resolution

MEETING DATE: **October 22, 2024**
FROM: **Michele Moore**
SUBJECT: **A Resolution of the City Commission of the City of Holly Hill, Florida, Establishing a "Not to Exceed" Price of $1,000,000 with Phillips & Jordan, Inc., for the Provision of Debris Hauling Services Following Hurricane Milton, Establishing a "Not to Exceed" Price of $400,000 with Tetra-Tech, Inc., for the Provision of Debris Monitoring Services Following Hurricane Milton, and Authorizing the City Manager to Execute the Same; Providing for Severability; and Providing for an Effective Date.**
NUMBER: **2024-R-85**
APPLICANT:
PLANNER:

Discussion:

On October 10th Hurricane Milton caused damage throughout the city. Immediately following the storm both City employee and City contractors began the clean-up process.

The City of Holly Hill has an agreement with Phillips and Jordan, Inc., for the provision of disaster debris hauling services through a one year contract extension to agreement RFP 19-PW-16. This extension agreement was approved by the Holly Hill City Commission on May 28, 2024, with the accompanying resolution, 2024-R-77, attached under 'Exhibit A' and is attached under 'Exhibit B'.

Similarly, the City of Holly Hill has an agreement with Tetra-Tech, Inc., for the provision of disaster debris monitoring services through a RFP 19-PW-15. This extension agreement was approved by the Holly Hill City Commission on May 25, 2024 with the accompanying resolution, 2024-R-77, also attached under 'Exhibit A' and is attached under 'Exhibit C'.

In an effort to remain in compliance with FEMA purchasing policies, and in order for purchase orders to be issued, "Not To Exceed" prices need to be established for each of these services.

The "Not To Exceed" prices recommended to be established for these agreements are as follows:

Debris Hauling: Phillips & Jordan, Inc., cost not to exceed $1,000,000.

Debris Monitoring: Tetra-Tech, Inc., cost not to exceed $400,000.

FISCAL ANALYSIS:

Based on previous storm experiences staff is recommending a budget amendment of $1,400,000.00 to cover the cost of storm related debris removal and debris removal monitoring. Funding for debris removal and monitoring will be from Solid Waste reserves and will be submitted to FEMA for reimbursement.

STAFF RECOMMENDATIONS:

Amend the Budget an estimated $1,400,000.00 as per attached 'Exhibit D'.

GOALS:

Goal #2: Enhance City aesthetics through beautification and maintenance of city property and public rights of way, consistent enforcement of zoning and property maintenance codes, and development of reasonable design standards and a corresponding process which is applicable to all new developments and business improvements in the city.

Goal #4: Provide proficient public health and safety services in terms of police and fire protection, water, storm water, waste water and solid waste management and disaster preparedness with a focus on intergovernmental collaboration, private sector partnerships, and utilization of technologies and proven innovations.

MOTION:

APPROVE ESTABLISHING A "NOT TO EXCEED" PRICE OF $1,000,000 WITH PHILLIPS & JORDAN, INC., FOR THE PROVISION OF DEBRIS HAULING SERVICES FOLLOWING HURRICANE MILTON, ESTABLISHING A "NOT TO EXCEED" PRICE OF $400,000 WITH TETRA-TECH, INC., FOR THE PROVISION OF DEBRIS MONITORING SERVICES FOLLOWING HURRICANE MILTON.

ATTACHMENTS:

- Exhibit A - APPROVED - Resolution 2024-R-35 - Debris Hauling and Monitoring Contract Renewals (2) (DOC)
- Exhibit B - Fully Executed - Phillips & Jordan Agreement - June 2024 (PDF)
- Exhibit C -Fully Executed - Tetra Tech, Inc. - May 2024 (PDF)
- Exhibit D - Budget Amendment Hurricane Milton (PDF)

Resolution No. 2024-85

A RESOLUTION OF THE CITY COMMISSION OF THE CITY OF HOLLY HILL, FLORIDA, ESTABLISHING A "NOT TO EXCEED" PRICE OF $1,000,000 WITH PHILLIPS & JORDAN, INC., FOR THE PROVISION OF DEBRIS HAULING SERVICES FOLLOWING HURRICANE MILTON, ESTABLISHING A "NOT TO EXCEED" PRICE OF $400,000 WITH TETRA-TECH, INC., FOR THE PROVISION OF DEBRIS MONITORING SERVICES FOLLOWING HURRICANE MILTON, AND AUTHORIZING THE CITY MANAGER TO EXECUTE THE SAME; PROVIDING FOR SEVERABILITY; AND PROVIDING FOR AN EFFECTIVE DATE.

A RESOLUTION OF THE CITY COMMISSION OF THE CITY OF HOLLY HILL, FLORIDA, ESTABLISHING A "NOT TO EXCEED" PRICE OF $1,000,000 WITH PHILLIPS & JORDAN, INC., FOR THE PROVISION OF DEBRIS HAULING SERVICES FOLLOWING HURRICANE MILTON, ESTABLISHING A "NOT TO EXCEED" PRICE OF $400,000 WITH TETRA-TECH, INC., FOR THE PROVISION OF DEBRIS MONITORING SERVICES FOLLOWING HURRICANE MILTON, AND AUTHORIZING THE CITY MANAGER TO EXECUTE THE SAME; PROVIDING SEVERABILITY; AND PROVIDING FOR AN EFFECTIVE DATE.

WHEREAS, the City has an active agreement with Phillips & Jordan, Inc., for the provision of disaster debris hauling services; and

WHEREAS, the City has an active agreement with Tetra-Tech, Inc., for the provision of disaster debris monitoring services; and

WHEREAS, "Not to Exceed" prices need to be established for both Phillips & Jordan, Inc., and Tetra Tech, Inc., in order to provide a fiscal limit for time and materials contracts.

NOW, THEREFORE, BE IT RESOLVED BY THE CITY COMMISSION OF THE CITY OF HOLLY HILL, FLORIDA:

SECTION 1. That the City Commission of the City of Holly Hill establish a not to exceed price of $1,000,000 with Phillips & Jordan for the provision of debris hauling services, and authorize the City Manager to execute the same.

SECTION 2. That the City Commission of the City of Holly Hill establish a not to exceed price of $400,000 with Tetra-Tech, Inc., for the provision of debris monitoring

services, and authorize the City Manager to execute the same.

SECTION 3. SEVERABILITY. If any section or portion of a section of this Resolution proves to be invalid, unlawful, or unconstitutional, it shall not be held to invalidate or impair the validity, force, or effect of any other section or part of this Resolution.

SECTION 4. EFFECTIVE DATE. This Resolution shall take effect immediately upon its adoption.

APPROVED AND AUTHENTICATED on this 22nd day of OCTOBER, 2024.

HOLLY HILL
FLORIDA

STAFF REPORT
CITY OF HOLLY HILL, FLORIDA

City Commission
Resolution

MEETING DATE: May 28, 2024
FROM: Antoine Khoury
SUBJECT: **A Resolution of the City Commission of the City of Holly Hill, Florida, Authorizing the City Manager to Execute the First of the (1) One-Year Extensions to Agreement RFP 19-PW-16 with Phillips & Jordan, Inc., Crowder Gulf Joint Venture, Inc., and Ceres Environmental Services, Inc., for Emergency Debris Hauling and Authorizing the City Manager to Execute the First of the (1) One-Year Extensions to Agreement RFP 19-PW-15 with Tetra Tech, Inc., Rostan Solutions, LLC and Thompson Consulting Services, LLC for Emergency Debris Monitoring; Providing for Severability; and Providing for an Effective Date.**
NUMBER: 2024-R-35
APPLICANT:
PLANNER:

DISCUSSION:

On June 11, 2019, the City Commission approved joint emergency debris hauling agreements with Phillips & Jordan Inc., Crowder Gulf Joint Venture, Inc and Ceres Environmental Services, Inc., and approved joint emergency debris monitoring agreements with Tetra Tech, Inc., Rostan Solutions, LLC and Thompson Consulting Services, LLC. These agreements have an initial term of five (5) years from the date of award with five (5) additional one (1) year renewal options. The initial terms of these agreements are set to expire on June 11, 2024. Although debris hauling and debris monitoring agreements were done as joint agreements with the City of South Daytona and the City of New Smyrna Beach, the terms of the agreement specify that each City retains the sole right to determine whether the renewal option should be granted. Copies of these agreements are included under Exhibit 'A'.

With the approach of hurricane season, it is imperative that the City maintain active agreements with both debris haulers and debris monitors should a disaster occur. All debris haulers and monitors have agreed to maintain current rates of their agreements. As such, it is recommended that Phillips & Jordan, Crowder Gulf and Ceres Environmental each be awarded the first of the one (1) year extensions for debris hailing and that Tetra Tech, Rostan Solutions and Thompson Consulting Services each be awarded the first of the one (1) year extensions for debris monitoring. Copies of these extension agreements are included under Exhibit 'B'.

FISCAL ANALYSIS:

Attachment: Exhibit A - APPROVED - Resolution 2024-R-35 - Debris Hauling and Monitoring Contract Renewals (2) (2024-R-85 : Debris Hauling

There are no costs affiliated with awarding one-year extensions to these contracts. Should a disaster occur, one debris hauler and one debris monitor will be activated and "not to exceed costs" will be developed and presented to the Holly Hill City Commission for approval.

STAFF RECOMMENDATION:

Staff recommends that the City Commission authorize the City Manager to execute the first of the (1) one-year extensions to agreement RFP 19-PW-16 with Phillips & Jordan, Inc., Crowder Gulf Joint Venture, Inc., and Ceres Environmental Services, Inc., for emergency debris hauling and authorize the City Manager to execute the first of the (1) one-year extensions to agreement RFP 19-PW-15 with Tetra Tech, Inc., Rostan Solutions, LLC and Thompson Consulting Services, LLC for emergency debris monitoring.

COMMISSION GOAL:

Goal #1: Develop and maintain a sound and sustainable financial plan for the city that establishes sufficient reserves for all funds, ensures (whenever possible) that user fees pay for services rendered, provides a realistic capital improvement program, and encourages public/private sector partnerships and intergovernmental partnerships.

MOTION:

Authorize the City Manager to execute the first of the (1) one-year extensions to agreement RFP 19Authorize the City Manager to execute the first of the (1) one-year extensions to agreement RFP 19-PW-16 with Phillips & Jordan, Inc., Crowder Gulf Joint Venture, Inc., and Ceres Environmental Services, Inc., for emergency debris hauling and authorize the City Manager to execute the first of the (1) one-year extensions to agreement RFP 19-PW-15 with Tetra Tech, Inc., Rostan Solutions, LLC and Thompson Consulting Services, LLC for emergency debris monitoring.

ATTACHMENTS:

- Exhibit A - Contractor Agreements (PDF)
- Exhibit B - Contract Renewals (PDF)

Attachment: Exhibit A - APPROVED - Resolution 2024-R-35 - Debris Hauling and Monitoring Contract Renewals (2) (2024-R-85 : Debris Hauling

Attachment: Exhibit A - APPROVED - Resolution 2024-R-35 - Debris Hauling and Monitoring Contract Renewals (2) (2024-R-85 : Debris Hauling

Resolution No. 2024-35

A RESOLUTION OF THE CITY COMMISSION OF THE CITY OF HOLLY HILL, FLORIDA, AUTHORIZING THE CITY MANAGER TO EXECUTE THE FIRST OF THE (1) ONE-YEAR EXTENSIONS TO AGREEMENT RFP 19-PW-16 WITH PHILLIPS & JORDAN, INC., CROWDER GULF JOINT VENTURE, INC., AND CERES ENVIRONMENTAL SERVICES, INC., FOR EMERGENCY DEBRIS HAULING AND AUTHORIZING THE CITY MANAGER TO EXECUTE THE FIRST OF THE (1) ONE-YEAR EXTENSIONS TO AGREEMENT RFP 19-PW-15 WITH TETRA TECH, INC., ROSTAN SOLUTIONS, LLC AND THOMPSON CONSULTING SERVICES, LLC FOR EMERGENCY DEBRIS MONITORING; PROVIDING FOR SEVERABILITY; AND PROVIDING FOR AN EFFECTIVE DATE.

A RESOLUTION OF THE CITY COMMISSION OF THE CITY OF HOLLY HILL, FLORIDA, AUTHORIZING THE CITY MANAGER TO EXECUTE THE FIRST OF THE (1) ONE-YEAR EXTENSIONS TO AGREEMENT RFP 19-PW-16 WITH PHILLIPS & JORDAN, INC., CROWDER GULF JOINT VENTURE, INC., AND CERES ENVIRONMENTAL SERVICES, INC., FOR EMERGENCY DEBRIS HAULING AND AUTHORIZING THE CITY MANAGER TO EXECUTE THE FIRST OF THE (1) ONE-YEAR EXTENSIONS TO AGREEMENT RFP 19-PW-15 WITH TETRA TECH, INC., ROSTAN SOLUTIONS, LLC AND THOMPSON CONSULTING SERVICES, LLC FOR EMERGENCY DEBRIS MONITORING; PROVIDING FOR SEVERABILITY; AND PROVIDING FOR AN EFFECTIVE DATE.

WHEREAS, the current agreements for emergency debris hauling and emergency debris monitoring are set to expire on June 11, 2024; and

WHEREAS, it is of paramount importance to have debris hauling and monitoring agreements in place in the event that disaster strikes; and

WHEREAS, the City of Holly Hill retains the sole right to determine whether renewal options should be granted; and

WHEREAS, all debris haulers from agreement RFP 19-PW-16 and all debris monitors from agreement RFP 19-PW-15 have agreed to the first of the (1) one-year extensions with no price increases.

NOW, THEREFORE, BE IT RESOLVED BY THE CITY COMMISSION

OF THE CITY OF HOLLY HILL, FLORIDA:

SECTION 1. That the City Commission does hereby approve the first of the (1) one-year extensions to agreement RFP 19-PW-16 with Phillips & Jordan, Inc., Crowder Gulf Joint Venture, Inc., and Ceres Environmental Services, Inc., for emergency debris hauling.

SECTION 2. That the City Commission does hereby approve the first of the (1) one-year extensions to agreement RFP 19-PW-15 with Tetra Tech, Inc., Rostan Solutions, LLC and Thompson Consulting Services, LLC. for emergency debris monitoring.

SECTION 3. SEVERABILITY. If any section or portion of a section of this Resolution proves to be invalid, unlawful, or unconstitutional, it shall not be held to invalidate or impair the validity, force, or effect of any other section or part of this Resolution.

SECTION 4. EFFECTIVE DATE. This Resolution shall take effect immediately upon its adoption.

APPROVED AND AUTHENTICATED on this 28th day of MAY, 2024.

Chris Via, Mayor 5/28/2024

Valerie Manning, City Clerk,CMC 5/28/2024

RESULT:	**ADOPTED [UNANIMOUS]**
MOVER:	Penny Currie, District 2 - Commissioner
SECONDER:	John C. Danio, District 3 - Commissioner
AYES:	Via, Penny, Currie, Danio, Johnson

Attachment: Exhibit A - APPROVED - Resolution 2024-R-35 - Debris Hauling and Monitoring Contract Renewals (2) (2024-R-85 : Debris Hauling

FIRST RENEWAL AGREEMENT

THIS FIRST RENEWAL AGREEMENT, dated this 5th day of June, 2024, is entered into by and between the **CITY OF HOLLY HILL, FLORIDA,** a political subdivision of the State of Florida, hereinafter referred to as "CITY"; and **PHILLIPS AND JORDAN, INCORPORATED,** a **foreign for-profit corporation** hereinafter referred to as **"CONTRACTOR."**

WITNESSETH

WHEREAS, the CITY and CONTRACTOR entered into an agreement dated June 11, 2019, pursuant to the Joint Procurement for Emergency Disaster Debris Hauling & Disposal Request for Proposal No. 19-PW-16, together with all exhibits, attachments, and addenda are incorporated into this agreement as if fully set forth herein (the "Agreement");

WHEREAS, the initial term of the Agreement was for a five (5) year period beginning June 11, 2019, and ending June 10, 2024; and

WHEREAS, pursuant to the terms of the Agreement there are five (5), one (1) year renewal options.

WHEREAS, the Parties agree and would like to exercise the first of these five (5), one (1) year renewal options

NOW, THEREFORE, in consideration of the mutual covenants and provisions contained herein, additional to those heretofore made, the Agreement is hereby modified as follows:

1. The WHEREAS clauses are incorporated herein as true and correct.

2. The Agreement is renewed of period from June 11, 2024, to June 10, 2025

3. That as a result of this first renewal there remain four (4), one year renewal options.

4. All other terms and conditions, not modified as set forth herein, of the Agreement are hereby reaffirmed in their entirety.

5. The parties agree that this First Renewal Option and all documents associated with the transaction contemplated herein may be executed by electronic signatures.

[THE REMAINDER OF THIS PAGE INTENTIONALLY LEFT BLANK]

Attachment: Exhibit B - Fully Executed - Phillips & Jordan Agreement - June 2024 (2024-R-85 : Debris Hauling and Monitoring Costs - Hurricane

ORIGINAL

IN WITNESS WHEREOF, the CITY and the CONTRACTOR have caused this FIRST RENEWAL to be executed below by their duly authorized representatives.

PHILLIPS AND JORDAN, INC.

BY: DocuSigned by: Morgan Pierce
2E2CED33513C4D1...

Morgan Pierce
(printed name)

TITLE: President, Power

DATE: 6/4/2024

CITY OF HOLLY HILL, FLORIDA

BY:

Joseph A. Forte
(printed name)

TITLE: City Manager

DATE: 6/5/2024

Attachment: Exhibit B - Fully Executed - Phillips & Jordan Agreement - June 2024 (2024-R-85 : Debris Hauling and Monitoring Costs - Hurricane

AGREEMENT FOR EMERGENCY DEBRIS MONITORING SERVICES

BETWEEN CITY OF HOLLY HILL, FL AND TETRA TECH, INC.

AMENDMENT NO. 1

THIS **CONTRACT AMENDMENT NO. 1** is by and between **City of Holly Hill, Florida** (hereinafter referred to as "CLIENT"), and **TETRA TECH, INC.** (hereinafter referred to as "CONTRACTOR").

WITNESSETH:

WHEREAS, CLIENT has entered into a Contract for Emergency Debris Monitoring Services with CONTRACTOR for a period of five (5) years beginning on June 11, 2019 through June 11, 2024 with the option to renew the contract term for five (five) additional one (1) year periods.

WHEREAS, CLIENT and CONTRACTOR desire to exercise the first renewal option for one (1) additional year.

NOW, THEREFORE, the parties hereby agree as follows:

1. **CONTRACT TERM**. The Contract is renewed from June 12, 2024 through June 11, 2025.

2. **MODIFICATIONS.** This Contract Amendment and the Contract, taken together, constitute the final agreement between CLIENT and CONTRACTOR. Any modification of or additions to the terms of this Contract Amendment or Contract must be in writing and executed by the parties.

IN WITNESS WHEREOF, the parties have duly executed this Contract Amendment written below.

City of Holly Hill, Florida

Name: Joseph A. Forte
Title: City Manager 5/25/2024

TETRA TECH, INC.

Name: Jonathan Burgiel
Title: Business Unit President

Attachment: Exhibit C -Fully Executed - Tetra Tech, Inc. - May 2024 (2024-R-85 : Debris Hauling and Monitoring Costs - Hurricane Milton)

Revision Date: 3/11/15

CITY OF HOLLY HILL
Budget Amendment Request
Fiscal Year 2024/2025

Requesting Department		Date
Solid Waste		10/22/202

TAKE FUNDS FROM ACCOUNT NUMBER:	ACCOUNT DESCRIPTION:	AMOUNT:
495-0000-389-1000	Carry forward	1,400,000.0
	Total	1,400,000.0

ADD FUNDS TO ACCOUNT NUMBER:		
495-3040-534-3400	Other contractual Services	1,400,000.0
	Total	1,400,000.0

Purpose of Transfer: (include as much detail as possible)

For commission Approval October 22, 2024
To appropriate funds for Hurricane Milton Debris Hauling, $1,000,000 and Debris Monitoring, $400,000.00

Note: Funds can only be transferred within the same fund and same department without requiring further commission action. In addition funds can only be expended after amendment is completed.

---------- Management Approvals----------

Department Head Signature _____ Date _____

City Manager Signature _____ Date _____

---------- For Finance Use Only ----------

Step 1: Finance Review

Finance Director Signature _____ Date _____

Step 2: Budget Adjustment Entry

Funds are available for this request? Yes No

HTE Group # _____

Employee Signature _____ Date _____

Attachment: Exhibit D - Budget Amendment Hurricane Milton (2024-R-85 : Debris Hauling and Monitoring Costs - Hurricane Milton)

HOLLY HILL
FLORIDA

STAFF REPORT
CITY OF HOLLY HILL, FLORIDA

City Commission
Resolution

MEETING DATE: October 22, 2024
FROM: Valerie Manning
SUBJECT: A Resolution of the City Commission of the City of Holly Hill, Florida, Authorizing the City Manager to Execute an Addendum to Agreement RFP 19-PW-16 with Phillips & Jordan, Inc., for Emergency Debris Hauling; Providing for Severability; and Providing for an Effective Date.
NUMBER: 2024-R-86
APPLICANT:
PLANNER:

DISCUSSION:

During the debris hauling operation of Hurricane Ian in 2022, there was confusion over the language in the contract with Phillips and Jordan as to how Leaners, Hangers, and stumps would be collected and billed. New Smyrna Beach corrected the language I their agreement in 2022. The City of Holly Hill would like to clarify the language in the agreement to avoid future conflict. The current contract had confusing language that allows for an interpretation that the leaners, hangers, and stumps are to be removed and hauled away. The new language states that the leaners, hangers, and stumps are removed and placed at the ROW for collection. There is additional language that allows for the cost of compaction of C&D materials at the DMS before it is brought to the land fill.

FISCAL ANALYSIS:

Costs associated with this amendment will be covered by the city's budget amendment for responding to the effects of Hurricane Milton and will be eligible for reimbursement from FEMA.

STAFF RECOMMENDATION:

Approve authorizing the City Manager to execute an addendum to agreement RFP 19-PW-16 with Phillips & Jordan, Inc., for emergency debris hauling.

COMMISSION GOAL:

Goal #2: Enhance City aesthetics through beautification and maintenance of city property and public rights of way, consistent enforcement of zoning and property maintenance codes, and development of reasonable design standards and a corresponding process which is applicable to all new developments and business improvements in the city.

Goal #4: Provide proficient public health and safety services in terms of police and fire protection, water, storm water, waste water and solid waste management and disaster

preparedness with a focus on intergovernmental collaboration, private sector partnerships, and utilization of technologies and proven innovations.

MOTION:

APPROVE AND AUTHORIZE THE CITY MANAGER TO EXECUTE AN ADDENDUM TO AGREEMENT RFP 19-PW-16 WITH PHILLIPS & JORDAN, INC., FOR EMERGENCY DEBRIS HAULING.

ATTACHMENTS:

- Addendum to Hurricane Debris 10.22.2024(PDF)

Resolution No. 2024-86

A RESOLUTION OF THE CITY COMMISSION OF THE CITY OF HOLLY HILL, FLORIDA, AUTHORIZING THE CITY MANAGER TO EXECUTE AN ADDENDUM TO AGREEMENT RFP 19-PW-16 WITH PHILLIPS & JORDAN, INC., FOR EMERGENCY DEBRIS HAULING; PROVIDING FOR SEVERABILITY; AND PROVIDING FOR AN EFFECTIVE DATE.

A RESOLUTION OF THE CITY COMMISSION OF THE CITY OF HOLLY HILL, FLORIDA, AUTHORIZING THE CITY MANAGER TO EXECUTE AN ADDENDUM TO AGREEMENT RFP 19-PW-16 WITH PHILLIPS & JORDAN, INC., FOR EMERGENCY DEBRIS HAULING, PROVIDING FOR SEVERABILITY; AND PROVIDING FOR AN EFFECTIVE DATE.

WHEREAS, the current agreements for emergency debris hauling and emergency debris monitoring were renewed by the City Commission on May 28, 2024; and

WHEREAS, the City and Contractor needed to clarify the fee schedule with regard to Leaners, Hangers, and Stumps and to include a compaction rate for C&D material.

NOW, THEREFORE, BE IT RESOLVED BY THE CITY COMMISSION OF THE CITY OF HOLLY HILL, FLORIDA:

SECTION 1. That the City Commission does hereby approve the addendum to agreement RFP 19-PW-16 with Phillips & Jordan, Inc., for emergency debris hauling attached hereto marked as Exhibit A.

SECTION 2. SEVERABILITY. If any section or portion of a section of this Resolution proves to be invalid, unlawful, or unconstitutional, it shall not be held to invalidate or impair the validity, force, or effect of any other section or part of this Resolution.

SECTION 3. EFFECTIVE DATE. This Resolution shall take effect immediately upon its adoption.

APPROVED AND AUTHENTICATED on this 22nd day of OCTOBER, 2024.

ADDENDUM TO
CONTRACTOR AGREEMENT
EMERGENCY DEBRIS HAULING & DISPOSAL
Request for Proposal (RFP) 19-PW-16.

THIS ADDENDUM TO AGREEMENT is made and entered into this _____ day of _____, 2024, by the CITY OF HOLLY HILL, a Municipal Corporation, hereafter referred to as the "City", and the PHILLIPS & JORDAN, INC., a for profit corporation, whose mailing address 10201 Parkside Drive, Suite 300, Knoxville, TN 37922, is hereinafter referred to as "CONTRACTOR."

The City and the Contractor agree to the following addendum to the agreement and the following section of the agreement is amended to read as follows:

Exhibit A
Attachment 1
Rate Schedules

5	Vegetative debris load and haul - from Right of Way/ Public Property to DMS or FDS	CY	$ 11.25
5	Removal of Eligible Hazardous Trees		
	Work consists of removing hazardous trees and placing debris on the ROW to be hauled under Item 5.1		
	6 inch to 12.99 inch diameter	EA	$ 45.00
	13 inch to 23.99 inch diameter	EA	$ 95.00
	24 inch to 35.99 inch diameter	EA	$135.00
	36 inch to 47.99 inch diameter	EA	$195.00
	48 inch and larger diameter	EA	$225.00
5	Removal of Eligible Hazardous Limbs - Per Tree		
	Work consists of removing (cutting) hazardous limbs greater than 2 in. in diameter from trees and placing debris on the ROW to be h	per tre	$112.50
5	Extraction of Eligible Hazardous Stumps		
	Work consists of removing hazardous stumps, backfill, transport DMS or Final Disposal.		
	Greater than 24 inch to 36.99 inch diameter	EA	$225.00
	37 inch to 48.99 inch diameter	EA	$250.00
	49 inch and larger diameter	EA	$275.00
6	Load and haul Construction and demolition debris, including white goods - from Right of Way/ Public Property to DMS or FDS	CY	$ 11.25
6	Load and haul reduced vegetative debris - from DMS to FDS *TBD by no later than 30 days after emergency event	CY	$ 10.50
6	Load and Haul of Compacted C & D mixed and other non-vegetative materials - from DMS to FDS) *TBD by no later than 30 days af	Per To	$ 37.00
6	Pass Thru Tipping Fees	CY/TN	At Cost
6.15	Grinding / Incinerating/Compacting	CY	$2.25

Except as above modified, all terms and conditions of the Agreement entered into between the City of Holly Hill and Contractor, shall remain unchanged and remain in full force and effect.

(Signature page to follow)

Attachment: Addendum to Hurricane Debris 10.22.2024 (2024-R-86 : Amendment to Agreement with Phillips & Jordan, Inc. for Emergency

CITY OF HOLLY HILL,
a Florida municipal corporation

By:

_____
Joseph A. Forte
City Manager

Date: _____

CITY OF HOLLY HILL,
a Florida municipal corporation

By: _____
Chris Via
Mayor

Date: _____

(City Seal)

Attest:

_____
Valerie Manning
City Clerk

Attachment: Addendum to Hurricane Debris 10.22.2024 (2024-R-86 : Amendment to Agreement with Phillips & Jordan, Inc. for Emergency

Phillips & Jordan, Inc.

By:

_____
Title:

Print Name: _____

Date: _____

Attest:

_____
Printed Name:_____
Title:_____

APPROVED AS TO FORM AND CORRECTNESS

_____
Scott Simpson
City Attorney

Date: _____

Attachment: Addendum to Hurricane Debris 10.22.2024 (2024-R-86 : Amendment to Agreement with Phillips & Jordan, Inc. for Emergency

HOLLY HILL
FLORIDA

STAFF REPORT
CITY OF HOLLY HILL, FLORIDA

City Commission
Agenda Item

MEETING DATE: October 22, 2024
FROM: Valerie Manning
SUBJECT: Fully Insured Group Insurance and Ancillary Lines of Coverage - January 1, 2025 - December 31, 2025
NUMBER: (ID # 4672)
APPLICANT:
PLANNER:

DISCUSSION:

Each year the City's agent of record, Brown and Brown, Employee Benefits Division solicits requests for proposals to carriers to provide group insurance coverage for the City of Holly Hill's eligible employees and retirees.

Based on the analysis of the insurance coverage options and rates received from these carriers, it is recommended by staff to bind coverage with the following carriers and plans:

Type of Coverage	Carrier	Est. Annual Premium	% Change
Health Insurance HDHP T95	Florida Health Care	$853,463	0.0%
Life Insurance	USAble	$28,803	4.7%
Dental Insurance (Employee-Paid)	Principal	$51,551	0.0%
Vision Insurance (Employee-Paid)	EyeMed	$6,879	0.0%

The City covers 100% of the cost of Health Insurance for the employee and the employee may elect to purchase coverage at their own expense for their eligible dependents. Life insurance is an employer-paid benefit which provides basic life with AD&D coverage for current employees and voluntary coverage is available, paid solely by employees; retirees are eligible to continue the previously City-paid basic life policy under the conditions of the policy and at their own expense. Dental and Vision insurance are voluntary coverages and the premiums are paid solely by the individual employee that elects to receive coverage.

FISCAL ANALYSIS:

The City's contribution on the behalf of each employee is fully funded within the 2024-2025 budget. The life insurance increase of 4.7% equates to $1,290/year and the City had not seen an increase for the 3 years prior despite several claims; we once again have a rate lock for 2 years.

STAFF RECOMMENDATION:

Authorize the City Manager to enter into a contract with Florida Health Care Plans, Principal Dental, EyeMed Vision and USAble Life to provide group benefit insurance for the plan year of 1/01/2025 to 12/31/2025 in accordance with the attached proposals.

COMMISSION GOAL:

Goal #1: Develop and maintain a sound and sustainable financial plan for the city that establishes sufficient reserves for all funds, ensures (whenever possible) that user fees pay for services rendered, provides a realistic capital improvement program, and encourages public/private sector partnerships and intergovernmental partnerships.

MOTION:

AUTHORIZE THE CITY MANAGER TO EXECUTE THE CONTRACTS WITH FLORIDA HEALTH CARE PLANS, INC., PRINCIPAL DENTAL, EYEMED VISION CARE, AND USABLE LIFE TO PROVIDE GROUP INSURANCE FOR THE PLAN YEAR OF JANUARY 1, 2025 TO DECEMBER 31, 2025.

- Benefits Rates Quote eff Jan 2025 - Final (PDF)



A Proposal of Employee Benefits
Coverage and Services

City of Holly Hill Employment Corporation

Jessica Scott
Sr. Vice President

Lauren Harbuck, GBDS
Account Executive

Mike Rusin, GBDS
Service Operations Leader

Hailey Cronk, GBDS
Sr. Brokerage Analyst

Proposal Date: October 14, 2024

Effective Date: January 01, 2025

Attachment: Benefits Rates Quote eff Jan 2025 - Final (4672 : Fully Insured Group Insurance and Ancillary

Brown & Brown

Brown & Brown is one of the largest and most respected independent insurance intermediaries in the nation, with over 70 years of continuous service. The Company is ranked as the sixth largest such organization in the United States by Business Insurance magazine.

Brown & Brown's clientele is as diverse as the American economy itself. There is hardly a business, industrial or professional insurance situation that has not presented itself to Brown & Brown including: Health/Medical, Retail, Construction, Marine, Transportation, e-Commerce, High Technology, Financial, Legal, Agricultural, Colleges and Universities, Golf Courses and Country Clubs, Governmental Entities, General Aviation, Hospitals, Hotels, Motels, Resorts, Manufacturing, Medical Care Facilities, Museums, Nursing Homes, Restaurants, Religious Institutions, Schools and many more.

Employee Benefits is just one area of expertise we can provide. Our benefit programs include Medical, Dental, Vision, Cobra, Life, Disability and Section 125 pre-tax reimbursement accounts just to name a few. We are able to provide fully insured programs for employers of all sizes and self-funded programs to meet the special needs of employers interested in that type of arrangement. In addition to providing the insurance programs, we assist in the design, cost-containment, management and development of your employee benefit package.

All Employee Benefit clients are assigned an "In House" service representative to assist with Billing, Claims, Eligibility, Enrollment, or any other issues or questions that arise.

For our clients that opt for self-insured programs, we not only provide the mentioned above, but also supply detailed reports to help you monitor your program closely. We also place the reinsurance, help design a plan to meet your needs and work closely with you and the Third Party administrator during the implementation as well as throughout the year to ensure the plan operates smoothly.

As for property and casualty, Brown & Brown is a recognized leader in the area of professional liability, governmental and municipal insurance programs, pollutions liability and many other specialized areas of risk. All property and casualty clients are assigned an "In-House" service representative along with a claims analyst to assist with daily issues, along with some of the best marketing representatives to search for the most competitive products and services our clients desire.

Commitment to Our Clients

The Employee Benefits Division at Brown & Brown of Florida, Inc. is focused on providing you with the best products at the most competitive rates possible. We ensure a very high level of customer service by remaining involved with you after the plan's effective date.

In addition to the Brown & Brown of Florida, Inc. Account Executive, all clients are assigned a team of dedicated service and marketing professionals committed to fast, efficient and friendly service during plan renewal and every other day of the year.

- We provide assistance with carriers to resolve any issues concerning policy administration, claims and billing.
- We provide expertise in designing, analyzing, and maintaining an employee benefits program that will help you attract and retain quality employees.
- We provide timely guidance on local and national trends in employee benefits and in the carrier marketplace.

As part of the 6th largest insurance broker in the country (as determined by Business Insurance magazine) we have the resources to partner with clients of all sizes and industries to maximize benefits and contain costs.
The Employee Benefits Division in Daytona Beach, FL is fully automated and highly efficient in marketing plan renewals and new business. We have access to all local and national carriers, third party administrators, and other specialists in the employee benefits industry including:

Medical · Dental · Vision · Life · Disability Plans · Cafeteria Plans · Self-funded and Partially Self-funded arrangements · Employee Assistance Programs · Voluntary (employee-paid) Long-Term Disability, Short-Term Disability, Dental and Accident & Sickness plans.

Phone
(800) 877-2769
(386) 252-9601

Address
Brown & Brown of Florida, Inc.
300 N Beach Street
Daytona Beach, FL 32114

Website
www.bbrown.com

NYSE Listed: BRO

Attachment: Benefits Rates Quote eff Jan 2025 - Final (4672 : Fully Insured Group Insurance and Ancillary

Disclaimer Information

The analysis of the following plans is a summary. You must refer to the contract and plan description for a full list of coverages and exclusions. In some instances broader coverage may be available. The rates and benefits in this proposal are based upon underwriting factors which included, but are not limited to, the census provided, the effective date shown, the status of employees/dependents (i.e. actively at work, COBRA, FMLA), final enrollment, etc. If any of the aforementioned changes prior to the proposed effective date, the final provisions, including rates, for these plans may vary or result in the proposed plan to be withdrawn. The rates shown are not guaranteed. Executive summaries are created by Brown & Brown of Florida, Inc. and neither the carrier nor Brown & Brown of Florida, Inc. will be held responsible for typographical or clerical errors. This proposal may not be a complete listing of all available benefit options. Different benefit levels may be available. This proposal is the proprietary work product of Brown and Brown of Florida, Inc. and is not authorized for further use or distribution. All insurance carriers have their own operating procedures. A change in carrier could affect certain benefits and coverage.

Brown and Brown of Florida, Inc. representatives are available to explain any items presented. It is assumed that the recipients of this proposal will seek an explanation of any items that may be in question. If coverage is moving to another carrier, please do not cancel your in force coverage until advised by Brown and Brown of Florida, Inc. Most carriers require a minimum of 30 days written notice to cancel coverage. Please check your policy contracts to be sure you meet the terms of your carrier cancellation provision and avoid duplicate coverage. The network provider/facility lists obtained via paper directories or carrier websites may contain providers and facilities that are no longer participating in the insurance carriers' networks. We cannot be responsible for any changes to the provider/facility listings that are not reflected. To ensure that a specific provider or facility is still participating in the provider's preferred network, we recommend contacting the provider/facility directly. For a current list, you may look on the Internet or call the toll-free number provided in each of the directories. Brown & Brown representatives may from time to time provide guidance regarding certain requirements affecting health plans, including the requirements of federal and state health care reform legislation. Such guidance is based on good-faith interpretation of laws and regulations currently in effect, and is not intended to be a substitute for legal advice. Employers should contact their own legal counsel for advice for legal requirements.

Failure to adhere to provisions of the Affordable Care Act (such as pay-or-pay, employer reporting requirements, benefit mandates, etc.) may result in significant fees and penalties to the employer. For a more comprehensive explanation of what fees and penalties may apply to you, you may contact your Brown and Brown of Florida, Inc. representative at any time. You are required to comply with Health Care Reform's Summary of Benefits & Coverage (SBC) distribution guidelines, which include requirements for SBC distribution at the plan renewal date. If an employee must enroll to continue coverage, the SBC must be provided when open enrollment materials are distributed. If enrollment materials are not distributed, employees must receive an SBC by the first day they are eligible to enroll. For insured plans, if coverage continues automatically for the next year, the SBC must be provided at least 30 days before the beginning of the new plan year. If the policy is not issued by that date, the SBC must be provided within seven business days once the information is available. Please refer to the Department of Health & Human Services' (HHS) official guidance for complete details regarding renewal and other SBC distribution guidelines.

Questions and Information Request:
Should you have any questions, or require additional information, please contact this office at 1-800-877-2769 or, if you prefer, submit your question or request online at http://www.bbinsurance.com/customerinquiry.shtml.

Compensation

Brown & Brown entities (“we”) receive commissions and fees from insurance carriers and other vendors as part of our compensation for placing and servicing your policies and products. Commissions are generally a percentage of the total premium and may be based on a schedule. In some cases, we may also receive direct compensation from the plan or the plan sponsor (service and/or consulting fees). Brown & Brown’s expected compensation (commissions and fees) for insurance products and related services placed on your behalf is hereby disclosed in the attached Addendum.

In addition to commissions and fees paid to Brown & Brown by insurance or reinsurance carriers or third-party vendors as mentioned above, Brown & Brown entities may also receive supplemental and/or bonus compensation from the carrier or vendor based on new sales volume or retention, for example. Such supplemental and/or bonus compensation may consist of guaranteed override income based on our agency’s business production and retention with the carrier or vendor, general agency fees, and/or sales or retention bonuses and is partially derived from your premium dollars, after being combined (or “pooled”) with the premium dollars of other insureds that have purchased similar types of coverage. Brown & Brown may not know in advance if such a supplemental and/or bonus payment will be made by a particular carrier or vendor, or the amount of any such payments until the underwriting year is closed. If we are unable to calculate the exact compensation that may be earned at the time of the contract, a formula with a good faith estimate of the expected amount will be provided in the attached Addendum. If the amount cannot be calculated or estimated at the time of this disclosure, we will indicate it as such on the Addendum & provide the information upon written request when available.

Brown & Brown entities may also receive invitations to programs sponsored and paid for by insurance carriers or other vendors to inform brokers regarding their products and services, including possible participation in company-sponsored events such as trips, seminars, and advisory council meetings, based upon the total volume of business placed with the carrier you select. We may also receive non-monetary compensation (including but not limited to the value of travel, meals and entertainment expenses associated with such meetings, gifts, tickets for sporting and entertainment events and awards). Such compensation allocated to your policy is not normally expected to equal or exceed a sum of $250.00 in aggregate, when all non-monetary compensation items received are combined. If non-monetary compensation is estimated to exceed $250.00 in aggregate, a good faith estimate will be included on the Addendum.

Brown & Brown entities may, on occasion, receive loans or credit from insurance companies. Additionally, in the ordinary course of our business, we may collect and remit premiums on behalf of the carrier or vendor and may earn and retain interest on premiums or administrative fees you pay from the date we receive them until the date remitted to the carrier or vendor.

If an intermediary is utilized in the placement of coverage, the intermediary may or may not be owned in whole or part by Brown & Brown, Inc. or its subsidiaries. Brown & Brown entities operate independently and are not required to utilize other companies owned by Brown & Brown, Inc., but routinely do so. In addition to providing access to the carrier or other vendor, the Wholesale Insurance Broker/Managing General Agent may provide additional services including, but not limited to: underwriting, quoting, plan implementation assistance, claims advocacy and eligibility administration services. . Compensation paid for those services is either derived from your premium payment, which may on average be up to 15% of the premium you pay for coverage and may include additional fees charged by the intermediary or is paid to the Wholesaler/Managing General Agent via override.

Questions and Information Requests. Should you have any questions, or require additional information, please contact this office at 386-252-9601 or, if you prefer, submit your question or request online at http://www.bbinsurance.com/customerinquiry/ .

Attachment: Benefits Rates Quote eff Jan 2025 - Final (4672 : Fully Insured Group Insurance and Ancillary

Attachment: Benefits Rates Quote eff Jan 2025 - Final (4672 : Fully Insured Group Insurance and Ancillary

NOTICE OF CARRIER FINANCIAL STATUS

Brown & Brown makes every attempt to place coverage with carriers rated A- or better* through AM Best (www.ambest.com), a national credit rating agency with a specific focus on the insurance industry. Because an AM Best rating is not required by the various state departments of insurance, there are many carriers in the Employee Benefits industry that elect not to participate in AM Best's rating process for various reasons. Therefore, Brown & Brown periodically places coverage with carriers rated less than A- or non-rated by AM Best.

Please be advised that Brown & Brown does monitor carriers rated less than A- or non-rated on an ongoing basis. However, because Brown & Brown cannot certify the financial soundness or stability of any insurance company or alternative risk transfer entity, or otherwise predict whether the financial condition of a company might improve or deteriorate, we encourage you to review the financial information for each carrier at AM Best's website (www.ambest.com), a state department of insurance website, the applicable carrier website and/or with your accountant, legal counsel and other advisors.

If you need assistance identifying the appliable issuing carriers for your current coverage, renewal coverage, or the coverage options being presented to you, please feel free to contact us at 386-252-9601 for assistance. Alternative quotes with an A- or better rated carrier may also be available upon your request.

*AM Best General Rating Guide

Financial Strength Rating	
A++, A+	Superior
A, A-	Excellent
B++, B+	Good
B, B-	Fair
C++, C+	Marginal
C, C-	Weak
D	Poor
E	Under Regulatory Supervision
F	In Liquidation
S	Suspended

Financial Size Category (in Thousands)			
Class I	Up to	$1,000	
Class II	$1,000	to	$2,000
Class III	$2,000	to	$5,000
Class IV	$5,000	to	$10,000
Class V	$10,000	to	$25,000
Class VI	$25,000	to	$50,000
Class VII	$50,000	to	$100,000
Class VIII	$100,000	to	$250,000
Class IX	$250,000	to	$500,000
Class X	$500,000	to	$750,000
Class XI	$750,000	to	$1,000,000
Class XII	$1,000,000	to	$1,250,000
Class XIII	$1,250,000	to	$1,500,000
Class XIV	$1,500,000	to	$2,000,000
Class XV	$2,000,000	or	Greater

Attachment: Benefits Rates Quote eff Jan 2025 - Final (4672 : Fully Insured Group Insurance and Ancillary

Carrier Requirements
Large Group (50 +)

Florida Health Care Plans

Submission deadline is 15th of month prior
Group questionnaire required
Minimum participation is 75% all eligible
Telemedicine: Doctor on Demand included, additional copays apply

Please Note:
If you are moving your coverage to a new carrier, please do not cancel your in force coverage until advised by Brown & Brown of Florida, Inc.. Most carriers require a minimum of 30 days written notice to cancel coverage (even if it is at the anniversary of the policy). Please check your policy contracts to be sure you meet the terms of your carrier cancellation provision to avoid duplicate coverage.

These deadlines represent the final date most carrier's will accept for the selected effective date, however it does not guarantee that implementation will be completed and ID cards will be delivered by the effective date.

FEDERAL COMPLIANCE WARNING

Summary Plan Descriptions (SPDs) Must Be Distributed to Your Plan Participants

The Problem

ERISA (the federal Employee Retirement Income Security Act) requires employers who are plan administrators of their group health plans to comply with 2 important requirements or risk potential penalties and possible audits:
1. Maintain and distribute Summary Plan Descriptions (SPDs) to plan participants which accurately reflect the contents of the plan and which include specific information as required under federal law.

2. Group health plans must be administered in accordance with a written Plan Document which must be made available to plan participants and beneficiaries upon request.

Many companies mistakenly assume that insurance contracts, certificates of insurance and benefits summaries fulfill the ERISA requirements for an SPD and Plan Document--but they don't include the required or recommended provisions that protect the plan and the employer.

Penalties for Non-Compliance

Employers/plan administrators may be liable for serious penalties if they don't provide an SPD or have a current Plan Document:
• Failure to provide an SPD or Plan Document within 30 days of receiving a request from a plan participant or beneficiary can result in a penalty of up to $110/day per participant or beneficiary for each violation.
• Lack of an SPD could trigger a plan audit by the U.S. Department of Labor (DOL).
• The DOL has increased its audit staff and national enforcement initiatives to investigate employers' compliance with Health Care Reform, resulting in companies of all sizes being audited and being required to provide an SPD and Plan Document.

The Solution

Typically, the cost to develop an SPD and Plan Document can be very expensive--but we have solved this problem with a sophisticated system developed together with a major ERISA law firm that makes it easy and economical to comply with federal requirements.

Brown & Brown Daytona Beach Retail will provide you with a Wrap SPD and Wrap Plan Document which are designed to wrap around existing certificates of insurance and benefit plan booklets to provide the required provisions and information necessary to comply with ERISA. To be compliant, the Wrap SPD and accompanying benefit plan component documents must be distributed to plan participants. Our document compliance solution includes the following benefits:
• Customized Wrap SPD and Wrap Plan Document that provide the required ERISA provisions and information that will help you achieve compliance.
• Distribution guidelines that explain how and when to provide these compliance documents to your plan participants.
• The ability to keep your documents current and updated should the federal government issue new amendments or if plan information needs to be changed.
PCP Plan Documents—IRS Requirement

A Premium Conversion Plan (PCP) is a type of cafeteria plan under Internal Revenue Code Section 125. It provides employees with an opportunity to make their required employee contributions for certain benefits on a pre-tax basis. Under the Code, a PCP must have a written plan document. If you provide this type of benefit to your employees and your business is audited by the IRS, this is one of the documents they will probably request. As part of our services, we can generate a PCP Plan Document and SPD to help you avoid adverse consequences in the event of an IRS audit.

Cost:
• ERISA Wrap Document & Summary Plan Description - $150
• Cafeteria Plan/Premium Conversion Plan - $50
• Updates/Summary of Material Modification - $100

Attachment: Benefits Rates Quote eff Jan 2025 - Final (4672 : Fully Insured Group Insurance and Ancillary

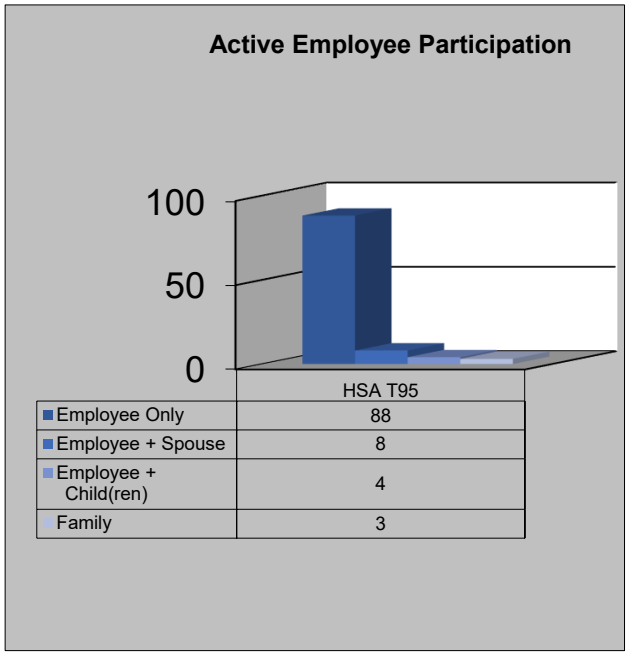
City of Holly Hill Employment Corporation

MEDICAL PARTICIPATION OVERVIEW

Enrollment Data	Current/Renewal
	HSA T95
Employee Only	88
Employee + Spouse	8
Employee + Child(ren)	4
Family	3
Total	**103**

Declining Medical (waivers only)	52
Participation	66.45%

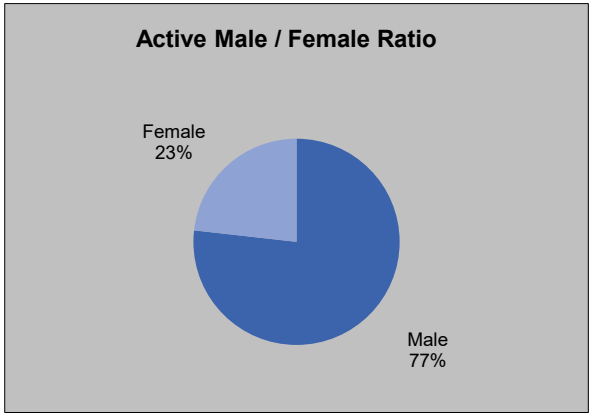
(participation does not include employees with other coverage)



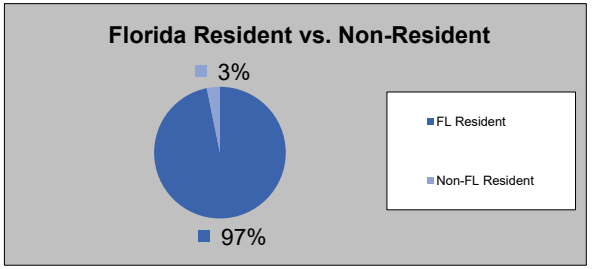
(Includes all employees)

Male	Female
119	36

Average Age
55



FL Resident	150
Non-FL Resident	5



Attachment: Benefits Rates Quote eff Jan 2025 - Final (4672 : Fully Insured Group Insurance and Ancillary

Executive Summary of Medical & Prescription Drug Coverage

City of Holly Hill
January 1, 2024 - December 31, 2024

	Current | Renewal | Revised
Vendor	Florida HealthCare Plans
Plan Name	HDHP T95
Network	Florida Healthcare Plans
Plan Type	POS - HSA
Plan Details	***Network***
	Single / ***Family***
Plan Deductible	$1,650 / $3,300
Embedded Deductible:	No
Calendar or Policy Year:	Calendar
Coinsurance:	20%
Maximum Out-of-Pocket:	$3,300 / $6,600
(Includes Deductible, Copay, Rx)	Yes | Yes | Yes
Physician Services	
Office Visit:	Deductible + Coinsurance
Specialist:	Deductible + Coinsurance
Chiropractic:	Deductible + Coinsurance
Virtual Visits:	Ded (PCP) | Ded + $30 (Mental Health)
Hospital / Emergency Services	
Inpatient Hospital Per Admission:	Deductible + Coinsurance
Emergency Room:	Deductible + Coinsurance
Urgent Care:	Deductible + Coinsurance
Outpatient Surgical Facility:	Deductible + Coinsurance
Ambulatory Surgery Center:	Deductible + Coinsurance
Diagnostic Services	
Lab & X-Ray Outpatient:	Deductible + Coinsurance
Advanced Imaging Services (MRI, MRA, PET, CT):	Deductible + Coinsurance
Prescription Drug	
Deductible:	Calendar Year Deductible
Prescription Tier:	$3 | $10 | $30 | $55 | 15% | 25%
Walgreens:	$15 | $15 | $35 | $60
Mail Order Prescription (90 Day Supply):	$6 | $27 | $87 | $162
Non-Network Plan Details	***Non-Network***
Plan Deductible	$2,800 / $5,600
Coinsurance:	40%
Maximum Out-of-Pocket:	$6,000 / $12,000
Per Occurrence Deductible (Inpatient/Outpatient):	N/A

Plan Rates | Current Enrollment		Current	Renewal	Revised
Employee:	88	$619.42	$659.68	$619.42
Employee + Spouse:	8	$1,059.22	$1,128.07	$1,059.22
Employee + Child(ren):	4	$1,059.22	$1,128.07	$1,059.22
Family:	3	$1,300.78	$1,385.33	$1,300.78
Estimated Monthly Premiums:	103	$71,122	$75,745	$71,122
Estimated Annual Premiums:		**$853,463**	**$908,936**	**$853,463**
PEPY		**$8,286**	**$8,825**	**$8,286**
Rate Change from Current (%):			6.5%	0.0%
Rate Change from Current ($):			$55,473	$0

Notes:

Rates subject to final enrollment and underwriting

Attachment: Benefits Rates Quote eff Jan 2025 - Final (4672 : Fully Insured Group Insurance and Ancillary

Executive Summary of Dental Coverage

City of Holly Hill
January 1, 2025 - December 31, 2025

		Current	
Vendor		Principal	
Network:		Principal	
Plan Name:		Vol PPO	
		Network	
Plan Details		***Single***	***Family***
Coinsurance Percentage (Preventive | Basic | Major | Ortho):		100% | 80% | 50% | 50%	
Deductible (Family Maximum):		$50	$150
Deductible Waived for Preventive:		Yes	
Calendar or Policy Year Maximum:		$5,000	
Orthodontic Lifetime Maximum:		$1,000	
Included Adult Ortho:		Yes	
Dental Services		***Benefit Level***	***Frequency***
Routine Exam & Cleaning:		Preventive	2 per year
Fluoride Treatment:		Preventive	2 per yr, under age 14
X-Ray (Bitewings):		Preventive	1 per year
X-Ray (Full Mouth):		Preventive	1 per 3 years
Sealants:		Preventive	1 per 3 yrs, under age 14
Fillings:		Basic	
Oral Surgery (Simple):		Basic	
Oral Surgery (Complex):		Basic	
Root Canal Therapy:		Basic	
Periodontal Scaling:		Basic	
Periodontal Surgery:		Basic	
Crowns:		Major	1 per 5 years
Bridges		Major	1 per 5 years
Dentures:		Major	1 per 5 years
Implants:		Major	1 per 5 years
Non-Network Details		***Non-Network***	
Coinsurance Percentage (Preventive | Basic | Major | Ortho):		100% | 80% | 50% | 50%	
Deductible (Family Maximum):		$50	$150
Deductible Waived for Preventive:		Yes	
Calendar Year Maximum:		$5,000	
Percent of UCR:		90th	
Waiting Periods:		None	
Late Entrant Penalties:		Not Permitted	
Allows Annual Open Enrollment:		Yes	
Included Rollover:		No	
Employer Contribution:		0%	
Participation Requirement:		Greater of 20% or 5 Lives	
Rate Guarantee:		1 Yr Remaining (01/01/2024 - 12/31/2025)	

Plan Rates | Current Enrollment		Current
Employee:	67	$32.67
Employee + Spouse:	16	$67.24
Employee + Child(ren):	9	$75.29
Family:	3	$117.85
Total:	95	
Estimated Monthly Premiums:		$4,296
Estimated Annual Premiums:		**$51,551**
PEPY		**$543**

Notes:

Attachment: Benefits Rates Quote eff Jan 2025 - Final (4672 : Fully Insured Group Insurance and Ancillary

Executive Summary of Vision Coverage

City of Holly Hill

January 1, 2025 - December 31, 2025

		Current
Vendor		Eyemed
Network		Eyemed Select
Plan Name		PPO Vision
Copays		***Network***
Exam:		$10
Materials:		$25
Contact Fitting & Follow-up:		up to $40
Frequencies		
Exams:		12 months
Lenses:		12 months
Frames:		24 months
Contacts:		12 months
Allowances		
Frames:		$100
Contact (Elective):		$115
Contact (Medically Necessary):		Covered in full
Non-Network Allowances		***Non-Network***
Exam:		up to $35
Single Vision:		up to $35
Bifocal:		up to $49
Trifocal:		up to $74
Frames:		up to $50
Contact (Elective):		up to $92
Contact (Medically Necessary):		up to $210
Employer Contribution:		0%
Participation Requirement:		10 enrolled
Rate Guarantee:		1 Yr Remaining (1/1/2022 - 12/31/2025)
Plan Rates | Current Enrollment		Current
Employee:	55	$4.86
Employee + Spouse:	17	$9.23
Employee + Child(ren):	8	$9.72
Family:	5	$14.26
Total:	85	
Estimated Monthly Premiums:		$573
Estimated Annual Premiums:		**$6,879**
PEPY		**$81**

Notes:

Attachment: Benefits Rates Quote eff Jan 2025 - Final (4672 : Fully Insured Group Insurance and Ancillary

Executive Summary of Group Life & AD&D Coverage

City of Holly Hill
January 1, 2025 - December 31, 2025

Basic Life:	7,165,000
AD&D:	7,165,000

		Current | Renewal		
Vendor		USAble		
Class Definition | Plan Details:		Benefit	Maximum	Guarantee Issue
Class 1:	Mayor & Commissioners	$20,000	$20,000	$20,000
Class 2:	Union Police Officers	1x's Salary	$50,000	$50,000
Class 3:	Union Firefighters	1x's Salary	$50,000	$50,000
Class 4:	Union EE's not eligible in another group	1x's Salary	$50,000	$50,000
Class 5:	Non-Union EE's w/ salaries >$49,000	1x's Salary	$100,000	$100,000
Class 6:	Non-Union EE's w/ salaries <$49,000	1x's Salary	$50,000	$50,000
Class 7:	City Manager	1x's Salary	$175,000	$175,000
Class 8:	Retirees who retired on or after to July 7, 2007	1x's Salary	$150,000	$150,000
Class 9:	Retirees who retired prior to July 7, 2007	1x's Salary	$150,000	$150,000
Plan Details (Dependent):				
Spouse:		$5,000	$5,000	$5,000
Child(ren) Benefit:		Birth - 6 Months		$1,000
Child(ren) Benefit:		6 Months - 26 Years		$2,500
Full-Time Student:			26 Years	
Reduction Schedule:		50% at age 75 (Class 1,2,3,4,5,6,7,8) 35% at age 65, 58% at age 70, 72% at age 75 (Class 9)		
Waiver of Premium:			Included	
Conversion:			Included	
Accelerated Death Benefit:			Included	
Seatbelt/Safe Driver Benefit:			Included (Classes 1-7)	
Actively at Work Provision:			Included	
Employer Contribution:			100%	
Participation Requirement:			100%	
Rate Guarantee:			2 Years (01/01/2025 - 12/31/2026)	

Plan Rates	Current	Renewal	Revised
Basic Life	$0.300	$0.327	$0.315
AD&D	$0.020	$0.020	$0.020
Dependent (Not included in premium)	$1.68	$1.68	$1.68
Estimated Monthly Premiums:	$2,293	$2,486	$2,400
Estimated Annual Premiums:	**$27,514**	**$29,835**	**$28,803**
Rate Change from Current (%):		8.4%	4.7%
Rate Change from Current ($):		$2,321	$1,290

Notes:

Attachment: Benefits Rates Quote eff Jan 2025 - Final (4672 : Fully Insured Group Insurance and Ancillary

Executive Summary of Voluntary Group Life & AD&D Coverage
City of Holly Hill
January 1, 2025 - December 31, 2025

	Current	
Vendor	USAble	
	Mayor, Commissioners, & All Other Eligible Employees	
Plan Details (Employee)		
Benefit (Increments of):	$10,000	
Not to Exceed:	5x's Salary	
Maximum Benefit:	$500,000	
Guarantee Issue:	$120,000	
Plan Details (Dependent)		
Spouse Benefit (Increments of):	$5,000	
Maximum Benefit:	$250,000	
Guarantee Issue:	$30,000	
Not to Exceed:	100% of thr employee's amount	
Child(ren) Benefit:	Birth - 6 Months	$1,000
Child(ren) Benefit:	6 Months - 26 Years	$2k, $4k, $6k, $8k, $10k
Full-Time Student:	26 Years	
Reduction Schedule:	50% at age 75	
Waiver of Premium:	Included	
Portability:	Included	
Accelerated Death Benefit:	Included	
Seatbelt/Safe Driver Benefit:	Included	
Actively at Work Provision:	Included	
Employer Contribution:	0%	
Participation Requirement:	25%	
Rate Guarantee:	1 Yr Remaining (01/01/2024 - 12/31/2025)	

Plan Rates per $1,000	Current	
	Employee	Spouse
Under 20	$0.072	$0.042
Age 20 - 24	$0.072	$0.042
Age 25 - 29	$0.082	$0.051
Age 30 - 34	$0.102	$0.068
Age 35 - 39	$0.146	$0.076
Age 40 - 44	$0.208	$0.085
Age 45 - 49	$0.330	$0.127
Age 50 - 54	$0.524	$0.195
Age 55 - 59	$0.806	$0.365
Age 60 - 64	$1.258	$0.560
Age 65 - 69	$2.184	$1.077
Age 70 - 74	$3.896	$1.077
Age 75 - 79	$7.634	$1.077
Age 80 - 84	$7.634	$1.077
Age 85 - 89	$7.634	$1.077
Age 90+	$7.634	$1.077
AD&D	$0.023	$0.023
Child	$0.225	
AD&D	$0.026	

Premium Calculation
Step 1: Benefit _____ / 1000 = _____ # Units
Step 2: # Units _____ x _____ Age-banded Rate = $_____ Premium Per Month

Attachment: Benefits Rates Quote eff Jan 2025 - Final (4672 : Fully Insured Group Insurance and Ancillary

HOLLY HILL
FLORIDA

STAFF REPORT
CITY OF HOLLY HILL, FLORIDA

City Commission
Resolution

MEETING DATE: October 22, 2024
FROM: Joseph Forte
SUBJECT: A Resolution of the City of Holly Hill, Florida, Awarding the Naming Rights Of the Building Located at 1060 Ridgewood Avenue to Florida Health Care Plans, Inc., Providing for Severability; Providing for Conflicting Resolutions; And Providing for an Effective Date.
NUMBER: 2024-R-78
APPLICANT:
PLANNER:

DISCUSSION:

The City and the Pictona has the right to designate the name of the building and facilities located at 1066 Ridgewood Avenue, Holly Hill, FL 32117 (the "Facility"). The City and Pictona have already entered into a real property lease agreement and a management services agreement for Facility previously known as the City Hall Annex.

Florida Health Care plan, Inc., would like to acquire the right to name the Facility from the Owner and Tenant in consideration of the foregoing and mutual promises set forth in the attached Agreement. Florida Health Care Plans, Inc., will be paying a fee to Pictona for the naming rights.

FISCAL ANALYSIS:

There is no financial impact to the City for the naming rights.

STAFF RECOMMENDATION:

To approve the Agreement and authorize the City Manager to execute the Agreement

COMMISSION GOAL:

Goal #3: Implement the CRA master plan with a focus on the best utilization of vacant properties and blighted properties in the city. Attention should also focus on infrastructure improvements within the district and strategies to encourage private investment and business retention.

Goal #5: Promote a small town city "branding" that focuses on the city's accessible staff and interactive use of technologies (i.e. city website), the city's business friendly approach to attract

and retain business, and the city's available open space, parks, and waterfront amenities that enhance the quality of life for citizens.

MOTION:

TO APPROVE THE AGREEMENT AND AUTHORIZE THE CITY MANAGER TO EXECUTE THE AGREEMENT.

ATTACHMENTS:

- Naming Rights Agreements to Protect the Brands - City of Holly Hill, Pictona and FHCP FINAL clean Oct. 22. 2024 (PDF)

HISTORY:

10/08/24	**City Commission**	**CONSENSUS TO BRING BACK TO NEXT CC MTG**

Mr. Forte informed the Mayor and City Commissioners that this item will be pulled and placed on the October 22, 2024 regular City Commission meeting.

Resolution No. 2024-78

A RESOLUTION OF THE CITY OF HOLLY HILL, FLORIDA, AWARDING THE NAMING RIGHTS OF THE BUILDING LOCATED AT 1060 RIDGEWOOD AVENUE TO FLORIDA HEALTH CARE PLANS, INC., PROVIDING FOR SEVERABILITY; PROVIDING FOR CONFLICTING RESOLUTIONS; AND PROVIDING FOR AN EFFECTIVE DATE.

A RESOLUTION OF THE CITY OF HOLLY HILL, FLORIDA, AWARDING THE NAMING RIGHTS OF THE BUILDING LOCATED AT 1060 RIDGEWOOD AVENUE TO FLORIDA HEALTH CARE PLANS, INC.; PROVIDING FOR SEVERABILITY; PROVIDING FOR CONFLICTING RESOLUTIONS; AND PROVIDING FOR AN EFFECTIVE DATE.

WHEREAS, City of Holly Hill is the Owner with an address of 1065 Ridgewood Avenue, Holly Hill, FL 32117; Pictona is the Tenant with an address of 1060 Ridgewood Avenue, Holly Hill, FL 32117, Florida; and, Florida Health Care Plan, Inc., is the Sponsor with an address of 2450 Mason Avenue, Daytona Beach, FL 32114; and

WHEREAS, the Tenant and the Owner has the right to designate the name of the building and facilities located at 1066 Ridgewood Avenue, Holly Hill, FL 32117 (the "Facility"); and

WHEREAS, Owner and Tenant have entered into a real property lease agreement and a management services agreement for Facility; and

WHEREAS, Sponsor would like to acquire the right to name the Facility from the Owner and Tenant; and

WHEREAS, in consideration of the foregoing and mutual promises set forth in the Agreement, and for other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged.

NOW, THEREFORE, BE IT RESOLVED BY THE CITY COMMISSION OF THE CITY OF HOLLY HILL, FLORIDA:

SECTION 1. That the City Commission authorizes the City Manager to execute the Naming Rights Agreement To Protect the Brands document.

SECTION 2. That if any section, subsection, sentence, clause, phrase, or portion of this resolution, or application hereof, is for any reason held invalid or unconstitutional by an Court, such portion or application shall be deemed a separate, distinct and independent provision, and such holding shall not affect the validity of the remaining portions or application hereof.

SECTION 3. That all Resolutions made in conflict with this Resolution are hereby repealed.

SECTION 4. That this Resolution shall become effective immediately upon its adoption.

APPROVED AND AUTHENTICATED on this 8th day of OCTOBER, 2024.

Attachment: Naming Rights Agreements to Protect the Brands - City of Holly Hill, Pictona and FHCP FINAL clean Oct. 22. 2024 (2024-R-78 : A

NAMING RIGHTS AGREEMENT TO PROTECT THE BRANDS

This Naming Rights Agreement ("Agreement") shall be effective as of the date last listed below ("Effective Date") is entered into by and between Pictona ("Tenant") with an address of 1060 Ridgewood Avenue, Holly Hill, FL 32117, City of Holly Hill ("Owner") with an address of 1065 Ridgewood Avenue, Holly Hill, FL 32117and Florida Health Care Plan, Inc. ("Sponsor") with an address of 2450 Mason Avenue, Daytona Beach, FL 32114 Owner and Sponsor are each sometimes referred to individually herein as a "Party," and collectively as the "Parties."

WHERAS, the Tenant and the Owner has the right to designate the name of the building and facilities located at 1066 Ridgewood Avenue, Holly Hill, FL 32117 (the "Facility");

WHEREAS, Owner and Tenant have entered into a real property lease agreement and a management services agreement for Facility.
WHEREAS, Sponsor would like to acquire the right to name the Facility from the Owner and Tenant;

NOW THEREFORE, in consideration of the foregoing and mutual promises set forth below, and for other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the Parities hereby agree as follows:

1. Definitions.

As used in this Agreement, the following terms have the following meanings.

(a) The term "BCBSA" means Blue Cross and Blue Shield Association.

(b) The term "BCBSA Marks" means any Blue Cross and Blue Shield names and symbols, including without limitation the word mark BLUE CROSS, the word mark BLUE SHIELD, the standard Blue Cross symbol (with the interior design element of the Vitruvian Man), the standard Blue Shield symbol (with the interior design element of the Staff of Asclepius), the solid Blue Cross symbol, and the solid Blue Shield symbol, and any other names or symbols incorporating any such names or symbols or the term BLUE and any applications or registrations therefore identified or set forth in the Naming Rights. For purposes of this Agreement, BCBSA Marks shall include the Florida Health Care Plan, Inc. names, symbols, and logos.

(c) The term "Facility" means the facility to be named under the Naming Rights.

(d) The term "Naming Rights" means the naming rights, and associated rights and obligations, given to the Sponsor set forth in Exhibit A to this Agreement.

(e) The term "BCBSA License Agreement" means the license agreement between BCBSA and Sponsor under which Sponsor has certain rights to use certain BCBSA Marks.

Attachment: Naming Rights Agreements to Protect the Brands - City of Holly Hill, Pictona and FHCP FINAL clean Oct. 22. 2024 (2024-R-78 : A

(f) The term "Sponsor Facility Name" means the name given to the Facility by Sponsor as set forth in the Naming Rights.

(g) The term "Sponsorship Commitment" means the sponsorship commitments set forth in Exhibit B to this Agreement.

(h) The term "Term" means the period starting from the Effective Date and continuing for the period or through such times set forth in Exhibit A to this Agreement or until termination (whichever is earlier).

2. Sponsorship.

(a) **Naming Rights**. Subject to the terms and conditions of this Agreement, during the Term, Sponsor shall fulfill the Sponsorship Commitment, and Owner and/or Tenant will honor and fulfill the Naming Rights. Without limitation to the Naming Rights, Owner and/or Tenant will refer to the Facility with the Sponsor Facility Name and use the Sponsor Facility Name in any applicable signage, websites, social media, or other ways in which the name of a facility would commonly be used or referenced; Owner and/or Tenant will require applicable third parties (including without limitation tenants or other users of the facilities, media users, and advertisers) to refer to the Facility with the Sponsor Facility Name, including without limitation in any future written contracts; and Owner and/or Tenant will use commercially reasonable efforts to encourage others to refer to the Facility with the Sponsor Facility Name. For clarity, Owner and/or Tenant may not make any use of any BCBSA Marks except as part of the Sponsor Facility Name.

(b) **Quality**. Owner and/or Tenant acknowledges the importance of maintaining high standards of quality in any goods or services that may be reasonably associated with the Sponsor Facility Name or is likely to be seen as emanating from the same source and agrees, during the Term, to maintain and follow standards of quality that are comparable within the industry with respect to the type, nature, or quality of any such goods or services for comparable facilities.

(c) **Exclusivity**. During the Term, Sponsor has exclusive naming rights on or within the Facility over any entities primarily providing competitive or related goods or services. Sponsor shall have exclusive rights to the programming and other services provided at Facility. No competitors of Sponsor may use the Facility for programming or other services at Facility.

3. BCBSA Marks.

(a) **Ownership**. Owner and/or Tenant acknowledges and agrees that BCBSA owns all rights in the BCBSA Marks, including without limitation any trademark rights, service-mark rights, associated goodwill, and other intellectual-property, proprietary, or intangible rights, and that any and all use of the BCBSA Marks inures to the benefit of BCBSA. Owner and/or Tenant further acknowledges and agrees that any use of BCBSA Marks under this Agreement is subject to the BCBSA License Agreement; and if the BCBSA License Agreement expires or terminates, either BCBSA or Sponsor may give written notice to Owner and/or Tenant of such expiration or termination, in which case Owner and/or Tenant must cease use of any BCBSA Marks.

Attachment: Naming Rights Agreements to Protect the Brands - City of Holly Hill, Pictona and FHCP FINAL clean Oct. 22. 2024 (2024-R-78 : A

(b) **Presentation and Use**. Sponsor has the right to approve the presentation and use of any applicable BCBSA Marks in signage, advertising, tickets, and other materials or items to ensure that the use and quality standards of the BCBSA Marks are maintained and that any such presentation or use is consistent with Sponsor's obligations under the BCBSA License Agreement. Without limitation to the generality of the foregoing, Sponsor has the right to temporarily reduce, or require Owner and/or Tenant to temporarily reduce, when feasible, the prominence of the applicable BCBSA Marks on signage and associated materials for events at the Facility that Sponsor deems to be potentially controversial or otherwise reflect negatively on the BCBSA Marks.

4. Termination.

(a) If Owner and/or Tenant breaches this Agreement, Sponsor may terminate this Agreement upon 30 days' written notice to Owner and Tenant, if such breach has not been cured within such 30 day period to the sole satisfaction of Sponsor.

(b) After the third (3rd) year of the Term, Sponsor has the right to terminate this Agreement without cause upon one hundred twenty (120) days prior written notice.

(c) Sponsor may terminate this Agreement immediately upon written notice to Owner and/or Tenant if any one or more of the following occurs:

(1) Owner and/or Tenant fails to meet any of the following criteria:

(i) None of the events that are Financial Stability Conditions are applicable to Owner and/or Tenant;

(ii) Owner and/or Tenant has not been convicted of a felony within the past three years;

(iii) Owner and/or Tenant does not have a reputation that through association would be likely to dilute or tarnish the unique value of any of the BCBSA Marks, in Sponsor's reasonable business judgment;

(iv) No impermissible use of or reference to any BCBSA Marks currently appears in any of Owner's and/or Tenant's public- or consumer-facing communications, including without limitation Owner's and/or Tenant's website; or

(v) Owner is not a National Competitor or an entity in dispute or litigation with BCBSA involving enforcement and protection of any of the BCBSA Marks;

(2) Owner and/or Tenant uses or permits the Facility to be used for or associated with activities or events likely to tarnish the reputation or value of the BCBSA Marks, such as a casino; or

(3) The BCBSA License Agreement expires or terminates.

Attachment: Naming Rights Agreements to Protect the Brands - City of Holly Hill, Pictona and FHCP FINAL clean Oct. 22. 2024 (2024-R-78 : A

(d) Upon the expiration or termination of this Agreement, Owner and/or Tenant must cease any and all use of any BCBSA Marks under this Agreement.

(e) In the event, the underlying lease by and between Owner and Tenant is terminated or otherwise expires this Agreement shall also co-terminate with no additional obligations of the parties.

5. Representations and Warranties.

Each of the parties represents and warrants to the other as follows:

(a) It has the full power and authority to execute and perform under this Agreement—including without limitation the absence of any duty or obligation that would prevent (or be put in breach or default by) such execution, delivery, or performance;

(b) It has investigated the facts pertaining to this Agreement as it deemed necessary;

(c) It has relied upon its own judgment, belief, knowledge, and understanding, after careful consultation with its own legal counsel concerning the legal effect of this Agreement; and

(d) It enters into this Agreement voluntarily in the absence of any fraud, mistake, duress, coercion, or undue influence.

6. Limitation of Liability.

IN NO EVENT SHALL EITHER PARTY BE LIABLE TO THE OTHER FOR ANY SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY KIND, INCLUDING WITHOUT LIMITATION LOSS OF PROFITS, HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN AN ACTION FOR CONTRACT, STRICT LIABILITY, TORT, NEGLIGENCE, OR OTHERWISE, WHETHER OR NOT THE PARTY HAD BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

7. General Provisions.

(a) **Modifications**. This Agreement may not be amended or modified except by a writing duly executed by the parties.

(b) **Binding Effect**. This Agreement contains the entire agreement between the parties and supersedes and replaces any and all prior or contemporaneous agreements or understandings, written or oral, with regard to the matters set forth herein. This Agreement will bind and inure to the benefit of each of the parties and their respective successors in interest. Except as expressly provided (including express mentions of BCBSA), this Agreement is not for the benefit of any person or entity not a party to this Agreement.

(c) **Interpretation**. In the language of this Agreement, the singular and plural numbers, and the masculine, feminine and neuter genders, include the others; and the conjunctive “and” and the disjunctive “or” include the other. Section,

paragraph, and other captions or headings are used in this Agreement as a matter of convenience and for reference—and do not affect the interpretation of this Agreement.

(d) **Ambiguities or Uncertainties**. This Agreement (and any ambiguities or uncertainties) will be equally and fairly interpreted without reference to the identity of the party preparing this Agreement, on the express understanding and agreement that the parties participated equally in the negotiation and preparation of the Agreement—or have had equal opportunity to do so. The parties each hereby waives the benefit of any statute or principle of law that provides that, in cases of uncertainty, language of a contract should be interpreted most strongly against the party who caused the uncertainty to exist.

(e) **Severability**. If any provision of this Agreement is held to be invalid or unenforceable under applicable law, that provision will be reformed and construed consistently with applicable law as nearly as possible to reflect the original intentions of this Agreement; and in any event, the remaining provisions of this Agreement will remain in full force and effect.

(f) **Waiver**. Any waiver of any breach or covenant of this Agreement must be in a writing duly executed by the Party waiving the breach. A waiver of a breach or covenant of this Agreement may not be construed to be a waiver of any succeeding breach or any other covenant, unless specifically and explicitly stated in the waiver.

(g) **Counterparts; Signatures**. This Agreement may be executed in counterparts, each of which may be deemed an original and all of which together will constitute a single instrument. In the execution of this Agreement and delivery of signatures, facsimile or scanned signatures will be treated as having the same effect as original signatures.

IN WITNESS WHEREOF, the parties to this Agreement execute this Agreement as of the date and year written below.

SPONSOR	**OWNER**
_____	_____
Signature	Signature
_____	_____
Printed Name	Printed Name
_____	_____
Title	Title
_____	_____
Date	Date

Attachment: Naming Rights Agreements to Protect the Brands - City of Holly Hill, Pictona and FHCP FINAL clean Oct. 22. 2024 (2024-R-78 : A

TENANT

_____
Signature

_____
Printed Name

_____
Title

_____
Date

Attachment: Naming Rights Agreements to Protect the Brands - City of Holly Hill, Pictona and FHCP FINAL clean Oct. 22. 2024 (2024-R-78 : A

EXHIBIT A
NAMING RIGHTS

Facility: Pictona's Activity Center located at 1060 Ridgewood, Holly Hill, Florida

Monument Sign shall be placed and maintained throughout the Term. The Monument Sign shall read "Florida Health Care Plans Activity Center at Pictona Holly Hill".

Term: Six (6) years

Attachment: Naming Rights Agreements to Protect the Brands - City of Holly Hill, Pictona and FHCP FINAL clean Oct. 22. 2024 (2024-R-78 : A

EXHIBIT B
SPONSORSHIP COMMITMENT

B.1. Sponsor will pay to Tenant a one-time amount of fifty thousand dollars ($ 50,000) dedicated to construction costs. FHCP reserves the right to request documentation of costs of construction.

B.2. Sponsor shall commit over the Term of this Agreement, in good and valuable consideration forty-five thousand seven hundred fifty dollars ($ 45,750) per year. Payment shall be to Tenant. This is in addition to the amounts previously committed by Sponsor and the additional funds committed by Sponsor's affiliate. Each annual payment shall be invoiced and all undisputed amounts paid to Tenant within thirty (30) days of receipt of invoice.

B.3. Tenant shall be responsible for building, maintaining, and updating the programming schedule to the satisfaction of Sponsor. Sponsor will provide educational programs.

B.4. Tenant shall develop and present a marketing plan within 30 days of the Effective Date to Sponsor with the objective of bringing attendance and awareness to the programs offered at Facility. Tenant shall actively promote Sponsor. Owner shall only use such materials as preapproved by Tenant.

Attachment: Naming Rights Agreements to Protect the Brands - City of Holly Hill, Pictona and FHCP FINAL clean Oct. 22. 2024 (2024-R-78 : A

HOLLY HILL
FLORIDA

STAFF REPORT
CITY OF HOLLY HILL, FLORIDA

City Commission
Resolution

MEETING DATE: October 22, 2024
FROM: Brian Walker
SUBJECT: A Resolution of the City Commission of the City of Holly Hill, Volusia County, Florida, Providing for a Temporary Waiver of Building Permit Fees for Anticipated Repairs to Building or Structural Damage Caused by Hurricane Milton; Providing for an Intent and Purpose of This Resolution; Providing for a Filing Period for Eligible Building Permit Applications; Providing for Severability; and Providing for an Effective Date.
NUMBER: 2024-R-87
APPLICANT:
PLANNER:

DISCUSSION:

A Resolution for a temporary waiver of building permit fees for anticipated repairs to building or structural damage caused by Hurricane Milton.

STAFF RECOMMENDATION:

Approve Resolution as submitted by staff.

MOTION:

APPROVING A TEMPORARY WAIVER OF BUILDING PERMIT FEES FOR ANTICIPATED REPAIRS TO BUILDING OR STRUCTURAL DAMAGE CAUSED BY HURRICANE MILTON; PROVIDING FOR AN INTENT AND PURPOSE OF THIS RESOLUTION; PROVIDING FOR A FILING PERIOD FOR ELIGIBLE BUILDING PERMIT APPLICATIONS.

Resolution No. 2024-87

A RESOLUTION OF THE CITY COMMISSION OF THE CITY OF HOLLY HILL, VOLUSIA COUNTY, FLORIDA, PROVIDING FOR A TEMPORARY WAIVER OF BUILDING PERMIT FEES FOR ANTICIPATED REPAIRS TO BUILDING OR STRUCTURAL DAMAGE CAUSED BY HURRICANE MILTON; PROVIDING FOR AN INTENT AND PURPOSE OF THIS RESOLUTION; PROVIDING FOR A FILING PERIOD FOR ELIGIBLE BUILDING PERMIT APPLICATIONS; PROVIDING FOR SEVERABILITY; AND PROVIDING FOR AN EFFECTIVE DATE.

A RESOLUTION OF THE CITY COMMISSION OF THE CITY OF HOLLY HILL, VOLUSIA COUNTY, FLORIDA; PROVIDING FOR A TEMPORARY WAIVER OF BUILDING PERMIT FEES FOR ANTICIPATED REPAIRS TO BUILDING OR STRUCTURAL DAMAGE CAUSED BY HURRICANE MILTON; PROVIDING FOR AN INTENT AND PURPOSE OF THIS RESOLUTION; PROVIDING FOR A FILING PERIOD FOR ELIGIBLE BUILDING PERMIT APPLICATIONS; PROVIDING FOR SEVERABILITY; AND PROVIDING FOR AN EFFECTIVE DATE.

WHEREAS, Hurricane Milton has caused extensive damage to properties within the geographic area of the City of Holly Hill; and

WHEREAS, the City Commission previously established a schedule of building permits fees by Resolution; and

WHEREAS, in order to expedite the repairs required as a result of the anticipated damage caused by Hurricane Milton and to provide relief to property owners suffering from hurricane related hardships, the City Commission desires to temporarily waive building permit fees for permit applications related to repairing such damage; and

WHEREAS, this Resolution is adopted pursuant to the Florida Municipal Home Rule Powers Act, Section 166.222, Florida Statutes, and the emergency powers vested in the City Commission pursuant to all applicable law; and

WHEREAS, the City Commission hereby finds that this Resolution is in the best interests of the citizens and businesses of the City of Holly Hill.

NOW, THEREFORE, BE IT RESOLVED BY THE CITY COMMISSION OF THE CITY OF HOLLY HILL, FLORIDA:

SECTION 1. Recitals. The foregoing recitals are hereby fully incorporated

herein by this reference and are deemed a material part of this Resolution.

SECTION 2. Intent and Purpose. It is the intent and purpose of this Resolution to only address building or structural damage directly caused by Hurricane Milton. This Resolution is not intended to apply to building permit applications filed with the City that are not related to repairing building or structural damage caused by Hurricane Milton. To the extent that a particular building or structure was substantially destroyed by Hurricane Milton and is beyond repair according to the City's building official, a new replacement building or structure on the same property as the substantially destroyed building or structure shall be considered a repair under this Resolution.

SECTION 3. Temporary Waiver of Building Permit Fees. The City Commission of the City of Holly Hill hereby provides that building permit fees are hereby waived for any building permit application filed with the City by an Owner/Builder only, related to repairing building or structural damage caused by Hurricane Milton. All such applications must be filed with the City's Building Department on or after October 10, 2024, but no later than December 1, 2024. Permit fees are not waived for a contractor obtaining a permit to do work for a 3rd party. For purposes of granting the building permit fee waiver, the building official or his or her designee shall be responsible for verifying that the repairs being permitted are directly related to damage caused by Hurricane Milton. Notwithstanding the fee waiver authorized by this Section, all building application, licensing, insurance, inspection, and other building permit conditions required by law shall apply.

SECTION 4. Severability. If any section or portion of a section of this Resolution proves to be invalid, unlawful, or unconstitutional, it shall not be held to invalidate or impair the validity, force, or effect of any other section or part of this Resolution.

SECTION 5. Effective Date. This Resolution shall take effect immediately upon its adoption.

APPROVED AND AUTHENTICATED on this 22nd day of OCTOBER, 2024.

HOLLY HILL
FLORIDA

STAFF REPORT
CITY OF HOLLY HILL, FLORIDA

City Commission
Ordinance

MEETING DATE: **October 22, 2024**
FROM: **Brian Walker**
SUBJECT: **FIRST READING - an Ordinance of the City of Holly Hill, Florida, Amending the Land Development Regulations, by Amending the Official Zoning Map to Designate the Property Described in Exhibit a from CC-1 (Commercial Corridor District) to Business Planned Unit Development (BPUD) (Business Planned Unit Development); Providing for Conflicting Ordinances; Providing for Severability; and Providing an Effective Date.**
NUMBER: **2024-O-3079**
APPLICANT: **Brian Walker**
PLANNER:

INTRODUCTION:

Consider an Ordinance enacting a rezone from CC-1 (Commercial Corridor District) to BPUD (Business Planned Unit Development), for approximately 1.544 acres located north of Mason Avenue, east of Daytona Avenue and South of 1st Street, approximately 430 feet west of Beach Street. The property has a commercial future land use. (Cobb Cole, Applicant).

BACKGROUND:

The Applicant is requesting a rezone in order to develop a 40 foot tall, indoor, climate-controlled storage facility having a footprint of 33,262 square feet. The applicant has submitted renderings, as well as a preliminary plan and landscape plan. The overall project area consists of 12 parcels, two of which are developed with a building and parking area. The existing building will be demolished. The parcels will be combined into one parcel prior to site development.

Site Information

Size of Property: The property consists of approximately 1.544 acres.

Survey & Legal Description: (Exhibit A)

Parcel Identification Numbers: Per Property Appraiser. (**Exhibits B1 and B2**)

General Location: See Location Map **(Exhibit C**)

Frontage: The property has approximately 420 feet of frontage along Mason Ave and 1st Street, and 167 feet along Daytona Avenue.

Access: Vehicular access will be from Mason Avenue and 1st Street.

Aerial Photography: (**Exhibit D**)

Existing Development: Most of the property is vacant, however there is a 4,479 square foot building with parking area on the east end of the property.

Future Land Use Designation: The current FLU designation is Commercial. (**Exhibit E**)

Zoning: Current Zoning is CC-1 (Commercial Corridor), and the proposed is zoning is BPUD (Business Planned Unit Development). (**Exhibit F**)

Floodplain Impacts: Based on floodplain map analysis the property is not flood prone. (**Exhibit G**)

Wetland Impacts: Based on aerial photos and County wetland map analysis, there no wetlands on the subject property.

Buffers: Buffering will be provided as shown on the Preliminary Development Plan.

Zoning and Land Uses

For zoning districts and future land uses that surround the subject parcel, see the attached sheet labeled " **Land Use and Zoning Table**."

Consistency with the Comprehensive Plan

A review of the goals, objectives and policies of the comprehensive plan was conducted to determine if the proposed rezone is consistent with the comprehensive plan. Staff finds that the requested rezone is consistent with the City's Comprehensive Plan with particular emphasis on the following:

The uses proposed within this Business Planned Unit Development (BPUD) zoning classification are compatible with the General Commercial future land use designation as well as with existing adjacent land uses.

Policy FLU 1.1.2 - the ratio of building floor area (FAR) for the General Commercial Development future land use designation shall not exceed 1.95. The proposed development FAR is 1.48.

Objective 1.9 – The City shall promote urban infill development and redevelopment in areas where public facilities and services are available.

Policy 1.9.1 – The City shall promote and encourage infill development on previously bypassed, vacant properties and redevelopment of underutilized properties.

Objective 2.1 – Concurrency: The City shall approve development only where it demonstrates that the impacts of such development do not degrade the established level-of-service standards for public facilities and services below acceptable levels.

Appropriateness of the Requested Zoning Category

In reviewing the appropriateness of the requested BPUD zoning designation, the Board of Planning and Appeals and City Commission, must consider the 8 specific criteria listed in Sec.

82-372 of the Land Development Regulations. The applicant has reviewed the criteria and provided a narrative in the attachment labeled as Rezoning Requirements.

It is staff's opinion that the requested rezone from CC-1 to BPUD is justified and appropriate for the area.

STAFF RECOMMENDATION:

ADOPT THE ORDINANCE ENACTING A REZONE FROM CC-1 (COMMERCIAL CORRIDOR DISTRICT) TO BPUD (BUSINESS PLANNED UNIT DEVELOPMENT), AND APPROVE THE ASSOCIATED WRITTEN DEVELOPMENT AGREEMENT AND PRELIMINARY DEVELOPMENT AND LANDSCAPE PLAN, FOR APPROXIMATELY 1.544 ACRES LOCATED NORTH OF MASON AVENUE, EAST OF DAYTONA AVENUE AND SOUTH OF 1ST STREET, APPROXIMATELY 430 FEET WEST OF BEACH STREET, AS LEGALLY DESCRIBED IN EXHIBIT "A".

ATTACHMENTS:

- 148 Mason Avenue Trip Generation (PDF)
- Geotechnical Report (PDF)
- PUD application with parcel information sheets (PDF)
- Rezoning Requirements (PDF)
- Concept Plan (rev 8-23-2024) (PDF)
- Landscape Plan (rev 8-23-2024) (PDF)
- Renderings and Elevation (PDF)
- Land Use and Zoning Table (PDF)
- Development Agreement (PDF)
- Exhibit A - Legal & Survey (PDF)
- Exhibit B1 - Charlesdale Assoc, Inc(PDF)
- Exhibit B2 - KBL Property Investments, LLC (PDF)
- Exhibit C - Location Map (PDF)
- Exhibit D - Aerial Map (PDF)
- Exhibit E - FLU Designation (PDF)
- Exhibit F - Current and Proposed Zoning (PDF)
- Exhibit G - Flood Map (PDF)

Ordinance No. 2024-3079

FIRST READING - AN ORDINANCE OF THE CITY OF HOLLY HILL, FLORIDA, AMENDING THE LAND DEVELOPMENT REGULATIONS, BY AMENDING THE OFFICIAL ZONING MAP TO DESIGNATE THE PROPERTY DESCRIBED IN EXHIBIT A FROM CC-1 (COMMERCIAL CORRIDOR DISTRICT) TO BUSINESS PLANNED UNIT DEVELOPMENT (BPUD) (BUSINESS PLANNED UNIT DEVELOPMENT); PROVIDING FOR CONFLICTING ORDINANCES; PROVIDING FOR SEVERABILITY; AND PROVIDING AN EFFECTIVE DATE.

AN ORDINANCE OF THE CITY OF HOLLY HILL, FLORIDA, AMENDING THE LAND DEVELOPMENT REGULATIONS, BY AMENDING THE OFFICIAL ZONING MAP TO DESIGNATE THE PROPERTY DESCRIBED IN EXHIBIT A FROM CC-1 (COMMERCIAL CORRIDOR DISTRICT) TO BUSINESS PLANNED UNIT DEVELOPMENT (BPUD) (BUSINESS PLANNED UNIT DEVELOPMENT); PROVIDING FOR CONFLICTING ORDINANCES; PROVIDING FOR SEVERABILITY; AND PROVIDING AN EFFECTIVE DATE.

WHEREAS, the City Commission of the City of Holly Hill, Volusia County, Florida, has adopted a comprehensive plan pursuant to, and in compliance with 163.3161 et. Seq., Florida Statutes; and

WHEREAS, the City Commission, as authorized by 163.3202, Florida Statutes, has enacted and does enforce the Land Development Regulations, based on, related to, and as a means to implement its adopted comprehensive plan; and

WHEREAS, the City Commission has determined that it is necessary to amend its Land Development Regulations as herein provided in order to more effectively implement its adopted comprehensive plan; and

WHEREAS, the City Commission has determined that the proposed amendment to the Land Development Regulations is consistent with its adopted comprehensive plan.

NOW, THEREFORE, BE IT ORDAINED BY THE CITY COMMISSION OF THE CITY OF HOLLY HILL, FLORIDA:

SECTION 1. The Official Zoning Map of the City of Holly Hill is hereby amended to designate the property described in **Attachment A** as BPUD (Business Planned Unit Development) pursuant to the provisions contained in the attached Development Agreement, as **Attachment B** and incorporated in this Ordinance by reference.

SECTION 2. Development of the property described in Attachment A shall conform to the Land Development Regulations of Holly Hill.

SECTION 3. If any section, subsection, sentence, clause, phrase, or portion of this Ordinance, or application hereof, is for any reason held invalid or unconstitutional by any Court, such portion or application shall be deemed a separate, distinct, and independent provision, and such holding shall not affect the validity of the remaining portions or application hereof.

SECTION 4. That all ordinances made in conflict with this Ordinance are hereby repealed.

SECTION 5. That this Ordinance shall be posted at City Hall as required by law.

SECTION 6. This ordinance shall become effective upon approval and adoption by the City Commission of Holly Hill.

APPROVED AND AUTHENTICATED on this 22nd day of OCTOBER, 2024 for first reading.

ATTACHMENT A

LEGAL DESCRIPTION:

PARCEL A:

LOT 5, BRITTON'S SUBDIVISION, ACCORDING TO THE PLAT THEREOF RECORDED IN MAP BOOK 9, PAGE 143, OF THE PUBLIC RECORDS OF VOLUSIA COUNTY, FLORIDA. LESS AND EXCEPT ANY PORTION LYING WITH THE STATE ROAD RIGHT OF WAY.

LOTS 4 AND 6, BRITTON SUBDIVISION, AS RECORDED IN PLAT AS RECORDED IN MAP BOOK 9, PAGE 143, OF THE PUBLIC RECORDS OF VOLUSIA COUNTY, FLORIDA. LESS AND EXCEPT ANY PORTION LYING WITHIN THE STATE ROAD RIGHT OF WAY.

LOTS 7 AND 8, BRITTON SUBDIVISION, AS RECORDED IN PLAT AS RECORDED IN MAP BOOK 9 PAGE 143, OF THE PUBLIC RECORDS OF VOLUSIA COUNTY, FLORIDA.

LOT 1, AND WESTERLY 24.9 FEET OF LOT 2, BLOCK A, SAULSBURY PLACE, ACCORDING TO THE MAP OR PLAT THEREOF AS RECORDED IN PLAT BOOK 6, PAGE 103, OF THE PUBLIC RECORDS OF VOLUSIA COUNTY, FLORIDA.

LOT 2, EXCEPT THE EAST 25.3 FEET AND THE WEST 24.9 FEET BLOCK A, SAULSBURY PLACE, ACCORDING TO THE MAP OR PLAT THEREOF AS RECORDED IN PLAT BOOK 6, PAGE 103, OF THE PUBLIC RECORDS OF VOLUSIA COUNTY, FLORIDA.

PARCEL B:

PARCEL 1:

LOT 6, EXCEPTING THE WESTERLY 9.0 FEET THEREOF AND EXCEPTING THE WESTERLY 30 FEET OF THE NORTHERLY 60.7 FEET THEREOF, SIMPSON SUBDIVISION AS PER MAP IN MAP BOOK 11, PAGE 131, AND EXCEPTING THAT PORTION DEEDED FOR STATE ROAD RIGHT OF WAY BEING MORE PARTICULARLY DESCRIBED IN WARRANTY DEED RECORDED OFFICIAL RECORDS BOOK 3899, PAGE 2533, OF THE PUBLIC RECORDS OF VOLUSIA COUNTY, FLORIDA.

PARCEL 2:

PART OF LOT ONE (1), SIMPSON'S SUBDIVISION, BEING A RESUBDIVISION OF A PORTION OF BLOCK THIRTY-SIX (36), MASON AND CARSWELL'S HOLLY HILL,

FLORIDA, AS PER MAP RECORDED IN MAP BOOK 11, PAGE 131, OF THE PUBLIC RECORDS OF VOLUSIA COUNTY, FLORIDA, DESCRIBED AS FOLLOWS: BEGINNING AT A POINT ON THE NORTHERLY RIGHT-OF-WAY LINE OF MASON AVENUE (60 FEET WIDE) AT THE DISTANCE OF 158.78 FEET MEASURED ALONG SAID RIGHT-OF-WAY LINE OF MASON AVENUE SOUTH 63 DEGREES 27 MINUTES 46 SECONDS WEST FROM THE SOUTHERLY END OF THE CURVED LINE WHICH CONNECTS THE NORTHERLY RIGHT-OF-WAY LINE OF MASON AVENUE WITH THE WESTERLY RIGHT-OF-WAY LINE OF NORTH BEACH STREET (ALSO KNOWN AS DIXIE HIGHWAY), SAID POINT OF BEGINNING ALSO BEING AT THE SOUTHWESTERLY CORNER OF PREMISES CONVEYED BY THE ATLANTIC REFINING COMPANY TO METROPOLITAN LIFE INSURANCE COMPANY, BY DEED DATED DECEMBER 15, 1952, AND RECORDED AMONG THE PUBLIC RECORDS OF VOLUSIA COUNTY, IN DEED BOOK 479, PAGE 202; FROM SAID POINT OF BEGINNING EXTENDING THENCE (1) ALONG SAID RIGHT-OF-WAY LINE OF MASON AVENUE, SOUTH 63 DEGREES 27 MINUTES 46 SECONDS WEST 138.88 FEET TO A POINT IN LINE OF OTHER LANDS CONVEYED BY THE ATLANTIC REFINING COMPANY TO R. C. WILLIAMS, THENCE (2) ALONG SAID OTHER LANDS CONVEYED BY THE ATLANTIC REFINING COMPANY TO R. C. WILLIAMS, NORTH 26 DEGREES 32 MINUTES 14 SECONDS WEST 197.67 FEET TO A POINT ON THE SOUTHERLY RIGHT-OF-WAY LINE OF RIVERSIDE PLACE; THENCE (3) ALONG SAID SOUTHERLY RIGHT-OF-WAY OF RIVERSIDE PLACE, NORTH 63 DEGREES 24 MINUTES EAST 138.87 FEET TO A POINT IN LINE OF OTHER LANDS OF THE ATLANTIC REFINING COMPANY; AND THENCE (4) PARTLY ALONG LINE OF OTHER LANDS OF THE ATLANTIC REFINING COMPANY AND PARTLY ALONG LINE OF LANDS OF METROPOLITAN LIFE INSURANCE COMPANY, SOUTH 26 DEGREES 32 MINUTES 14 SECONDS EAST 197.83 FEET TO THE PLACE OF BEGINNING.

ALSO, BEGINNING AT A POINT ON THE NORTHERLY RIGHT-OF-WAY LINE OF MASON AVENUE (60 FEET WIDE) THE DISTANCE OF 297.66 FEET MEASURED ALONG SAID RIGHT-OF-WAY LINE OF MASON AVENUE SOUTH 63 DEGREES 27 MINUTES 46 SECONDS WEST FROM THE SOUTHERLY END OF THE CURVED LINE WHICH CONNECTS THE NORTHERLY RIGHT-OF-WAY LINE OF MASON AVENUE WITH THE WESTERLY RIGHT-OF-WAY LINE OF NORTH BEACH STREET (ALSO KNOWN AS DIXIE HIGHWAY), SAID POINT OF BEGINNING ALSO BEING AT THE SOUTHWESTERLY CORNER OF OTHER LANDS CONVEYED BY THE ATLANTIC REFINING COMPANY TO R. C. WILLIAMS; FROM SAID POINT OF BEGINNING EXTENDING THENCE (1) ALONG SAID RIGHT-OF-WAY LINE OF MASON AVENUE SOUTH 63 DEGREES 27 MINUTES 46 SECONDS WEST 150 FEET TO A POINT AT THE SOUTHWESTERLY CORNER OF SAID LOT NO. 1 OF "THE SIMPSON SUBDIVISION"; THENCE (2) ALONG THE WESTERLY LINE OF SAID LOT NO. 1 NORTH 26 DEGREES 30 MINUTES WEST 197.50 FEET TO A POINT ON THE SOUTHERLY RIGHT-OF-WAY LINE OF RIVERSIDE PLACE AT THE NORTHWESTERLY CORNER OF SAID LOT NO. 1, THENCE (3) ALONG SAID SOUTHERLY RIGHT-OF-WAY LINE OF RIVERSIDE PLACE, NORTH 63 DEGREES 24 MINUTES EAST 149.87 FEET TO A POINT IN LINE OF SAID OTHER LANDS CONVEYED BY THE ATLANTIC REFINING COMPANY TO R. C.

WILLIAMS, AND THENCE (4) ALONG SAID LINE OF OTHER LANDS CONVEYED TO R. C. WILLIAMS SOUTH 26 DEGREES 32 MINUTES 14 SECONDS EAST 197.67 FEET TO THE PLACE OF BEGINNING.

EXCEPTING FROM THE ABOVE-DESCRIBED PARCEL, THAT PORTION DEEDED FOR STATE ROAD RIGHT-OF-WAY BEING MORE PARTICULARLY DESCRIBED IN WARRANTY DEED RECORDED IN OFFICIAL RECORDS BOOK 3899. PAGE 2533, OF THE PUBLIC RECORDS OF VOLUSIA COUNTY, FLORIDA.

PARCEL C:

PARCEL 1:

THE EASTERLY 25.3 FEET OF LOT TWO (2) AND THE WESTERLY 25 FEET OF LOT THREE (3), AS MEASURED ALONG FIRST STREET, BLOCK "A", SAULSBURY'S PLACE, A SUBDIVISION OF BLOCK 36, MASON AND CARSWELL'S HOLLY HILL, AS PER MAP THEREOF IN MAP BOOK 6, PAGE 103, OF THE PUBLIC RECORDS OF VOLUSIA COUNTY, FLORIDA.

AND

THE EAST 3/4 OF LOT 3, BLOCK "A", SAULSBURY PLACE, HOLLY HILL, AND INCLUDING WEST 30 FEET OF NORTH 60 FEET OF LOT 6, SIMPSON SUBDIVISION, BLOCK 36, MASON AND CARSWELL'S HOLLY HILL AS PER MAP THEREOF IN MAP BOOK 11, PAGE 131, OF THE PUBLIC RECORDS OF VOLUSIA COUNTY, FLORIDA.

AND

PARCEL 2:

LOT TWO (2), BRITTON SUBDIVISION, PER MAP IN MAP BOOK 9, PAGE 143, OF THE PUBLIC RECORDS OF VOLUSIA COUNTY, FLORIDA, AND ALSO THE WESTERLY 9 FEET OF LOT ELEVEN (11), AND THE WESTERLY 9 FEET OF THE SOUTH 1/2 OF LOT TWELVE (12), BLOCK 36, MASON AND CARSWELL'S HOLLY HILL, PER MAP RECORDED IN MAP BOOK 2, PAGE 90, OF THE PUBLIC RECORDS OF VOLUSIA COUNTY, FLORIDA, AND LOT THREE (3), BRITTON'S SUBDIVISION OF THE SOUTH 1/2 OF LOT NINE (9), AND ALL OF LOT TEN (10), BLOCK 36, MASON AND CARSWELL'S HOLLY HILL, ACCORDING TO THE MAP RECORDED IN BOOK 9, PAGE 143, OF THE PUBLIC RECORDS OF VOLUSIA COUNTY, FLORIDA.

LESS AND EXCEPT THAT PORTION TAKEN BY ORDER OF TAKING RECORDED APRIL 25, 1994 IN OFFICIAL RECORDS BOOK 3914, PAGE 427, OF THE PUBLIC RECORDS OF VOLUSIA COUNTY, FLORIDA, DESCRIBED AS FOLLOWS:

THAT PART OF LOTS 2 AND 3, BRITTON'S SUBDIVISION, AS RECORDED IN MAP BOOK 9, PAGE 143, AND LOT 6, THE SIMPSON SUBDIVISION, AS RECORDED IN MAP BOOK 11, PAGE 131, OF THE PUBLIC RECORDS OF VOLUSIA COUNTY, FLORIDA IN SECTION 37, TOWNSHIP 15 SOUTH, RANGE 33 EAST, DESCRIBED AS FOLLOWS:

COMMENCE AT THE 3" IRON PIPE MARKING THE NORTHWEST CORNER OF LOT 8, OF SAID BRITTON'S SUBDIVISION; THENCE SOUTH 25°20'46" EAST, ALONG THE EAST LINE OF DAYTONA AVENUE, 136.53 FEET TO THE SOUTHWEST CORNER OF LOT 6, OF SAID BRITTON'S SUBDIVISION; THENCE NORTH 64°29'54" EAST ALONG THE EXISTING NORTHERLY RIGHT-OF-WAY LINE OF STATE ROAD 430, A DISTANCE OF 200.00 FEET TO THE SOUTHWEST CORNER OF LOT 3, OF SAID BRITTON'S SUBDIVISION FOR THE POINT OF BEGINNING; THENCE NORTH 25°20'46" WEST ALONG THE WEST LINE OF SAID LOT 3, A DISTANCE OF 37.71 FEET TO A POINT OF INTERSECTION WITH A NON-TANGENT CURVE, CONCAVE SOUTHEASTERLY, HAVING A RADIUS OF 7,685.56 FEET, AND A CHORD BEARING NORTH 63°13'46" EAST; THENCE NORTHEASTERLY ALONG THE ARC OF SAID CURVE THROUGH A CENTRAL ANGLE OF 00°21'14", A DISTANCE OF 47.47 FEET TO A POINT OF REVERSE CURVATURE WITH A CURVE, CONCAVE NORTHWESTERLY, HAVING A RADIUS OF 11,414.38 FEET, AND A CHORD BEARING NORTH 63°16'40" EAST; THENCE NORTHEASTERLY ALONG THE ARC OF SAID CURVE THROUGH A CENTRAL ANGLE OF 00°15'32", A DISTANCE OF 51.56 FEET TO THE POINT OF INTERSECTION WITH THE EAST LINE OF THE WEST 9.00 FEET OF LOT 6, OF SAID THE SIMPSON SUBDIVISION; THENCE SOUTH 25°20'46" EAST ALONG SAID EAST LINE, 39.86 FEET TO THE EXISTING NORTHERLY RIGHT-OF-WAY LINE OF STATE ROAD 430; THENCE SOUTH 64°29'54" WEST ALONG SAID EXISTING NORTHERLY RIGHT-OF-WAY LINE, 99.00 FEET, TO THE POINT OF BEGINNING.

148 MASON AVENUE

The City of Holly Hill
Volusia County, Florida

TRIP GENERATION REPORT

March 19, 2024

Prepared By:
Parker Mynchenberg and Associates, Inc.
Professional Engineers * Land Planners * Landscape Architects
1729 Ridgewood Avenue
Holly Hill, Florida 32117
386-677-6891



Attachment: 148 Mason Avenue Trip Generation (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

148 MASON AVENUE

The following calculations are based on the Institute of Transportation Engineers (ITE) 11th Edition
The trip generation for Mini - Warehouse (151).

Proposed Building Square Area = **32,500** **SF**
Proposed Building Square Area = **32.5** **/1000 SF**

T = # of Trips
X = 1,000 SF Gross Floor Area

Average Vehicle Trips Ends vs: Square Footage

Summary	
Weekday Daily =	47.13 tpd
Weekday A.M. Peak =	5.85 tph
Weekday P.M. Peak =	5.85 tpd
Saturday Daily =	57.53 tpd
Saturday Hourly =	5.53 tph
Sunday Daily =	48.75 tpd
Sunday Hourly =	6.50 tph

Weekday

Equation:	In	Out
T = average rate = 1.45	50%	50%
T = 47.13 tpd	23.56	23.56

Weekday: A.M. Peak Hour of Generator

Equation:	In	Out
T = average rate = 0.18	19%	81%
T = 5.85 tph	1.11	4.74

Weekday: P.M. Peak Hour of Generator

Equation:	In	Out
T = average rate = 0.18	64%	36%
T = 5.85 tph	3.74	2.11

Saturday

Equation:	In	Out
T = average rate = 1.77	50%	50%
T = 57.53 tpd	28.76	28.76

Saturday: Peak Hour of Generator

Equation:	In	Out
T = average rate = 0.17	54%	46%
T = 5.53 tph	2.98	2.54

Sunday

Equation:	In	Out
T = average rate = 1.5	50%	50%
T = 48.75 tpd	24.38	24.38

Sunday: Peak Hour of Generator

Equation:	In	Out
T = average rate = 0.2	49%	51%
T = 6.50 tph	3.19	3.32

Attachment: 148 Mason Avenue Trip Generation (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

Land Use: 151
Mini-Warehouse

Description

A mini-warehouse is a building in which a number of storage units or vaults are rented for the storage of goods. They are typically referred to as “self-storage” facilities. Each unit is physically separated from other units, and access is usually provided through an overhead door or other common access point.

Additional Data

The technical appendices provide supporting information on time-of-day distributions for this land use. The appendices can be accessed through either the ITETripGen web app or the trip generation resource page on the ITE website (https://www.ite.org/technical-resources/topics/trip-and-parking-generation/).

The sites were surveyed in the 1980s, the 1990s, the 2000s, and the 2010s in California, Colorado, Massachusetts, Minnesota, Nevada, New Jersey, Texas, and Utah.

Source Numbers

212, 403, 551, 568, 642, 708, 724, 850, 868, 876, 1024, 1035

Attachment: 148 Mason Avenue Trip Generation (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

Mini-Warehouse
(151)

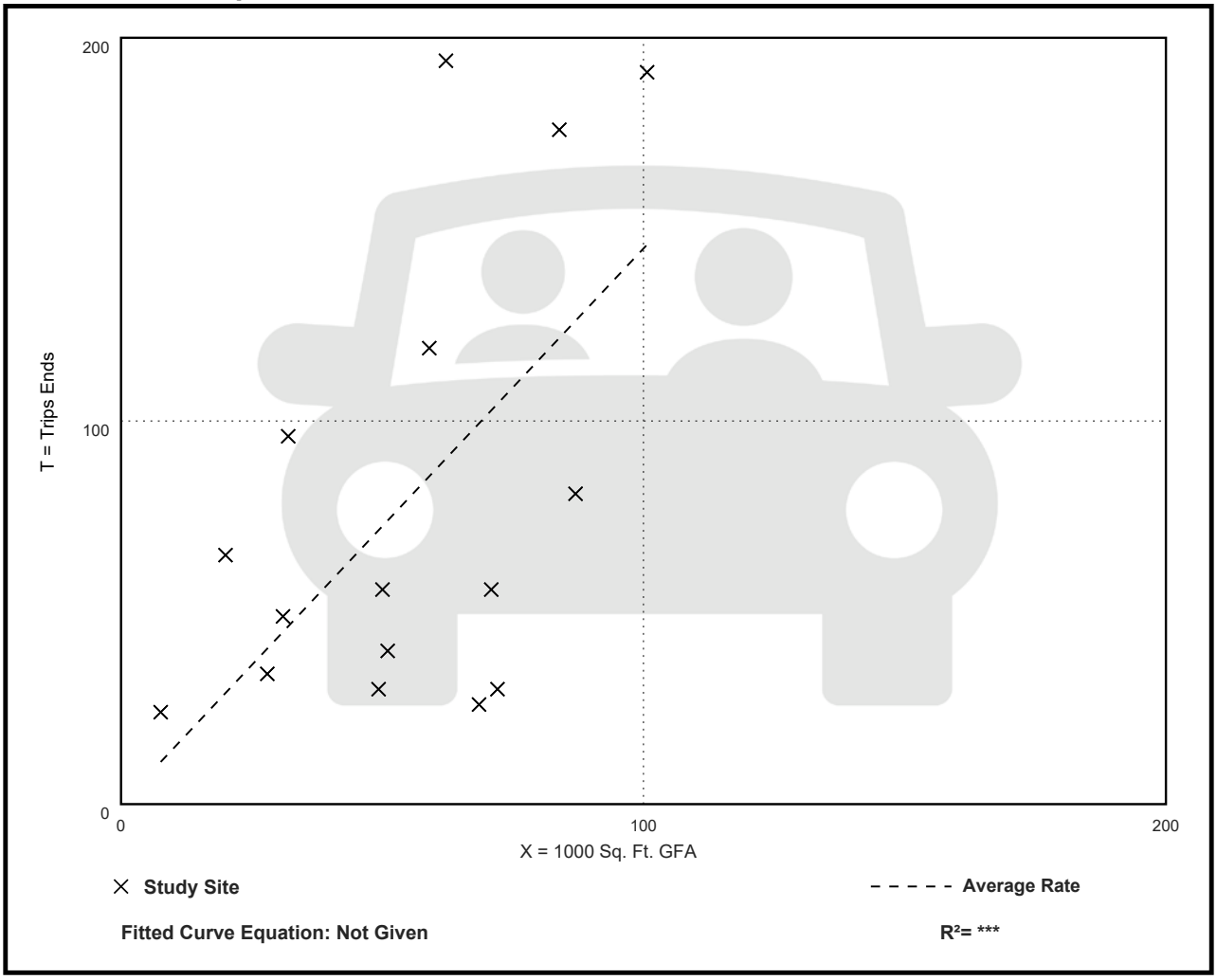
Vehicle Trip Ends vs: 1000 Sq. Ft. GFA
On a: Weekday

Setting/Location: General Urban/Suburban
Number of Studies: 16
Avg. 1000 Sq. Ft. GFA: 55
Directional Distribution: 50% entering, 50% exiting

Vehicle Trip Generation per 1000 Sq. Ft. GFA

Average Rate	Range of Rates	Standard Deviation
1.45	0.38 - 3.25	0.92

Data Plot and Equation



Attachment: 148 Mason Avenue Trip Generation (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

Mini-Warehouse
(151)

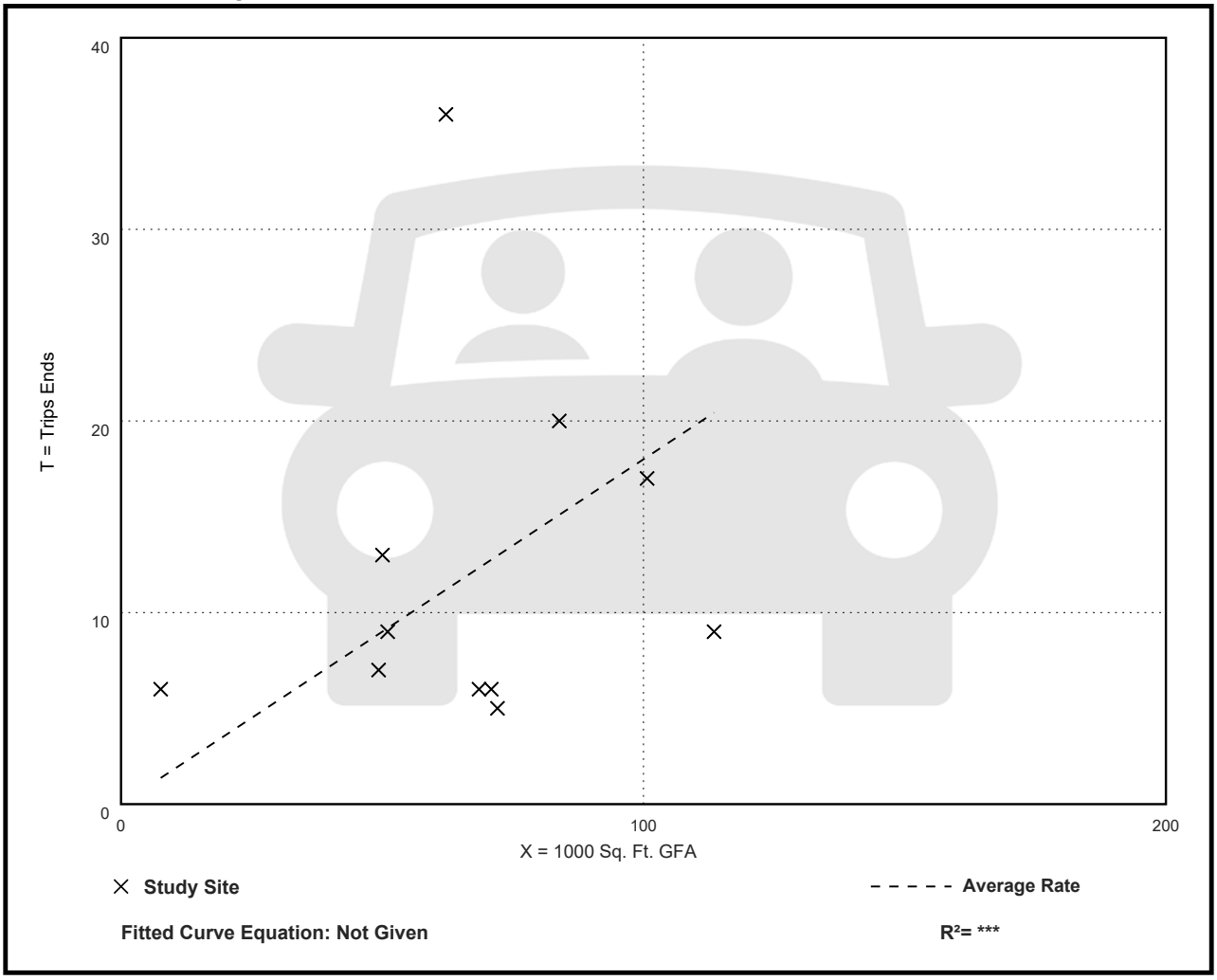
Vehicle Trip Ends vs: 1000 Sq. Ft. GFA
On a: Weekday,
AM Peak Hour of Generator

Setting/Location: General Urban/Suburban
Number of Studies: 11
Avg. 1000 Sq. Ft. GFA: 66
Directional Distribution: 51% entering, 49% exiting

Vehicle Trip Generation per 1000 Sq. Ft. GFA

Average Rate	Range of Rates	Standard Deviation
0.18	0.07 - 0.79	0.16

Data Plot and Equation



Attachment: 148 Mason Avenue Trip Generation (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

Mini-Warehouse
(151)

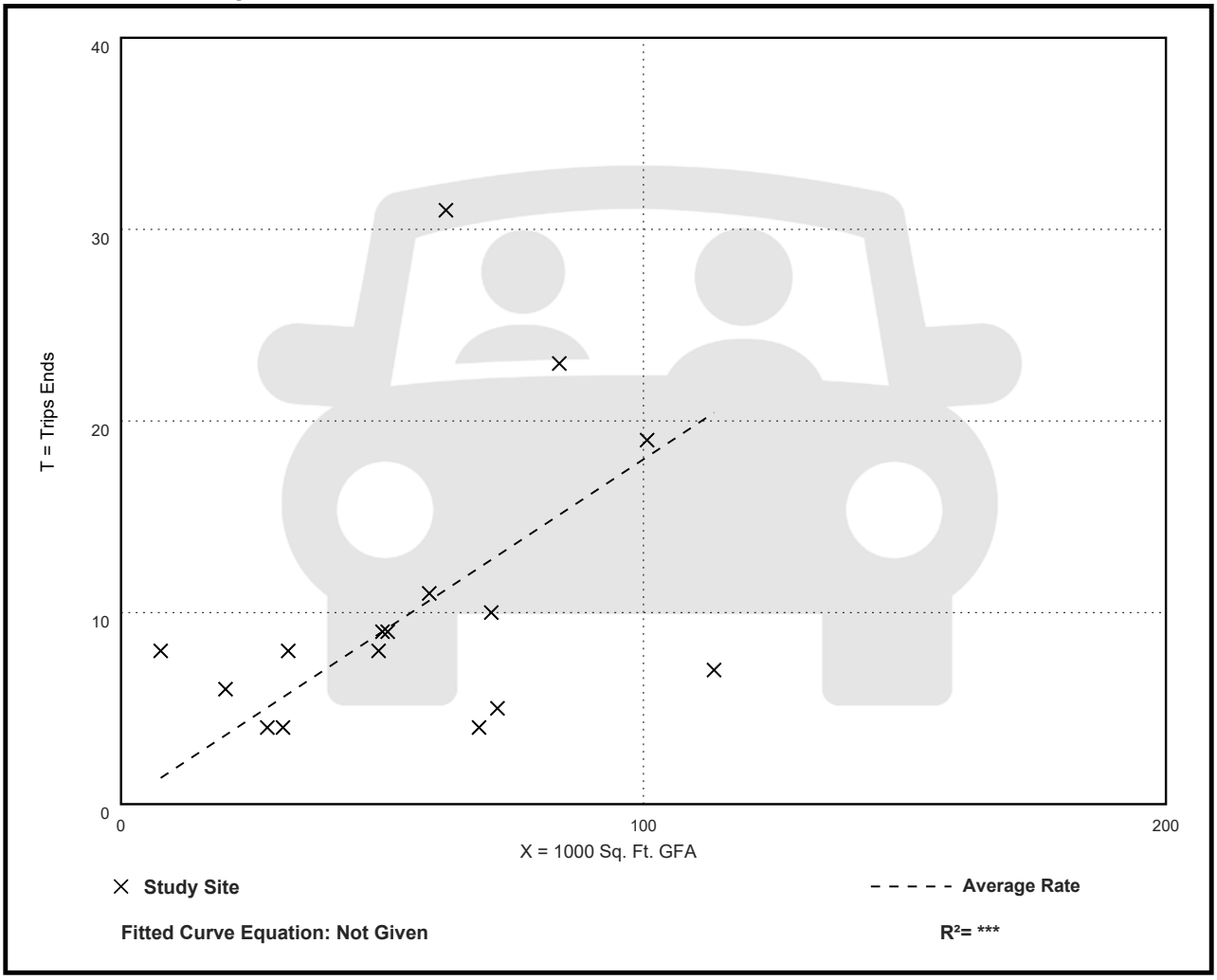
Vehicle Trip Ends vs: 1000 Sq. Ft. GFA
On a: Weekday,
PM Peak Hour of Generator

Setting/Location: General Urban/Suburban
Number of Studies: 16
Avg. 1000 Sq. Ft. GFA: 56
Directional Distribution: 51% entering, 49% exiting

Vehicle Trip Generation per 1000 Sq. Ft. GFA

Average Rate	Range of Rates	Standard Deviation
0.18	0.06 - 1.05	0.14

Data Plot and Equation



Attachment: 148 Mason Avenue Trip Generation (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

Mini-Warehouse
(151)

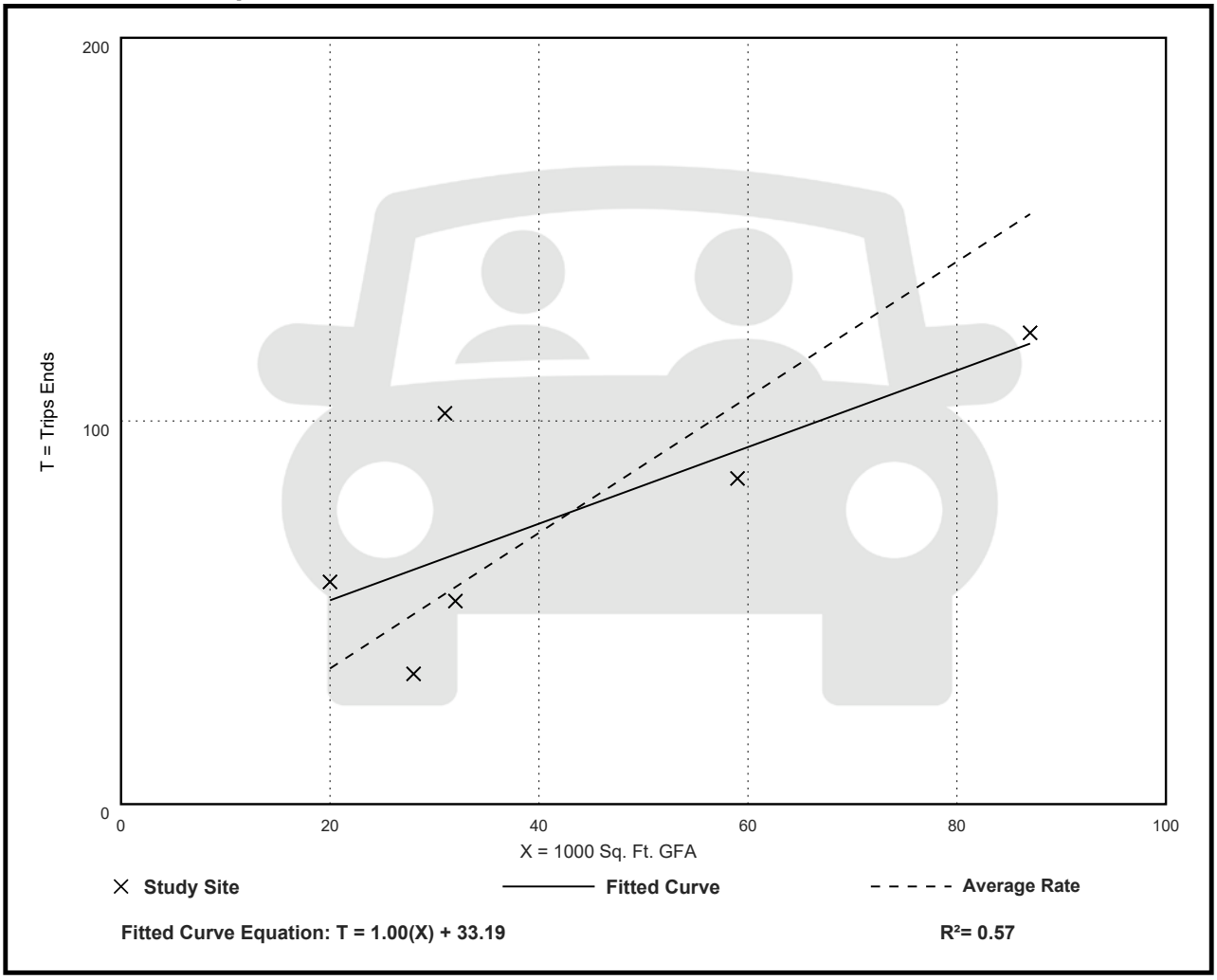
Vehicle Trip Ends vs: 1000 Sq. Ft. GFA
On a: Saturday

Setting/Location: General Urban/Suburban
Number of Studies: 6
Avg. 1000 Sq. Ft. GFA: 43
Directional Distribution: 50% entering, 50% exiting

Vehicle Trip Generation per 1000 Sq. Ft. GFA

Average Rate	Range of Rates	Standard Deviation
1.77	1.21 - 3.29	0.76

Data Plot and Equation



Fitted Curve Equation: T = 1.00(X) + 33.19

R^2= 0.57

Attachment: 148 Mason Avenue Trip Generation (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

Mini-Warehouse
(151)

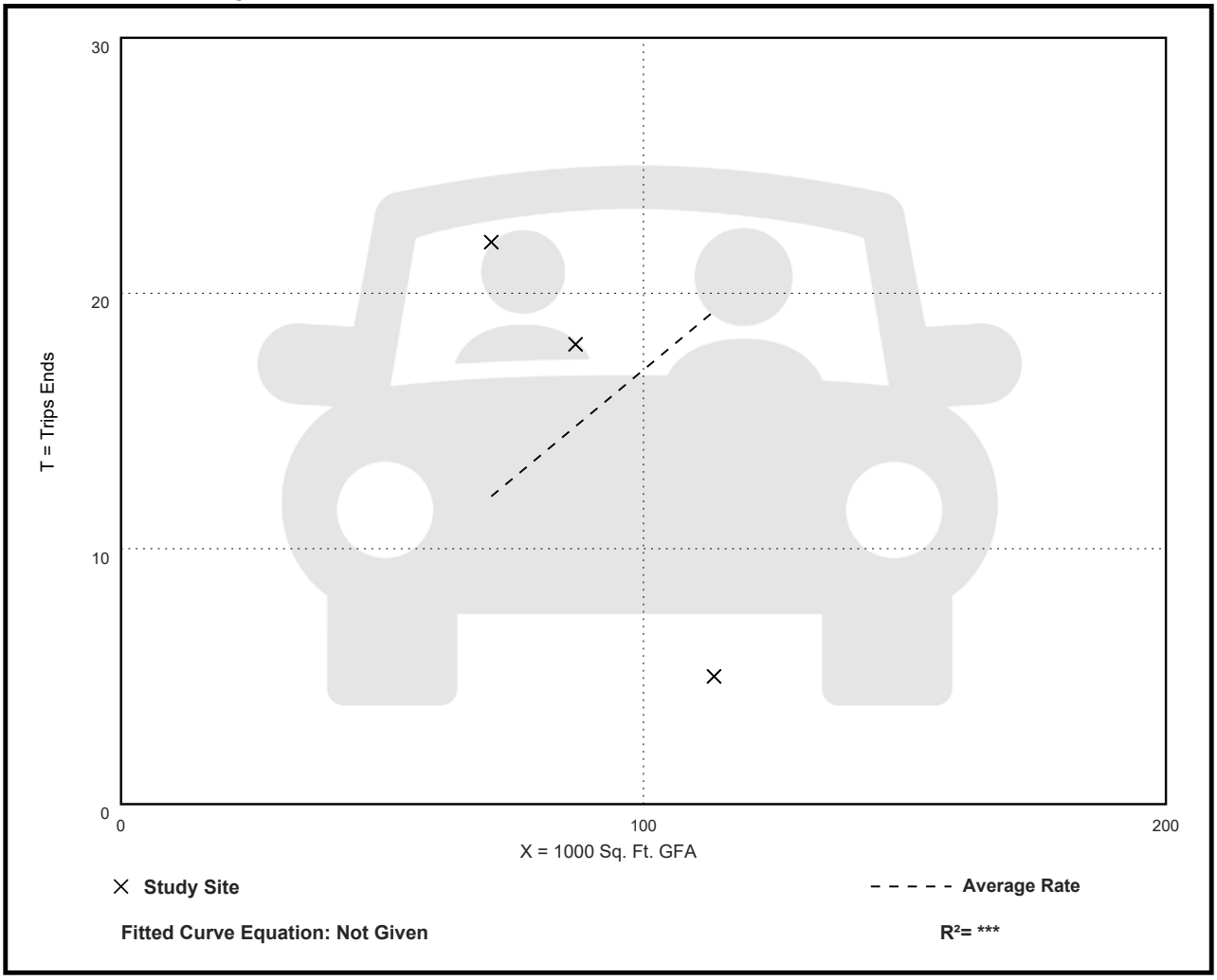
Vehicle Trip Ends vs: 1000 Sq. Ft. GFA
On a: Saturday, Peak Hour of Generator

Setting/Location: General Urban/Suburban
Number of Studies: 3
Avg. 1000 Sq. Ft. GFA: 90
Directional Distribution: 62% entering, 38% exiting

Vehicle Trip Generation per 1000 Sq. Ft. GFA

Average Rate	Range of Rates	Standard Deviation
0.17	0.04 - 0.31	0.14

Data Plot and Equation



Attachment: 148 Mason Avenue Trip Generation (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

Mini-Warehouse
(151)

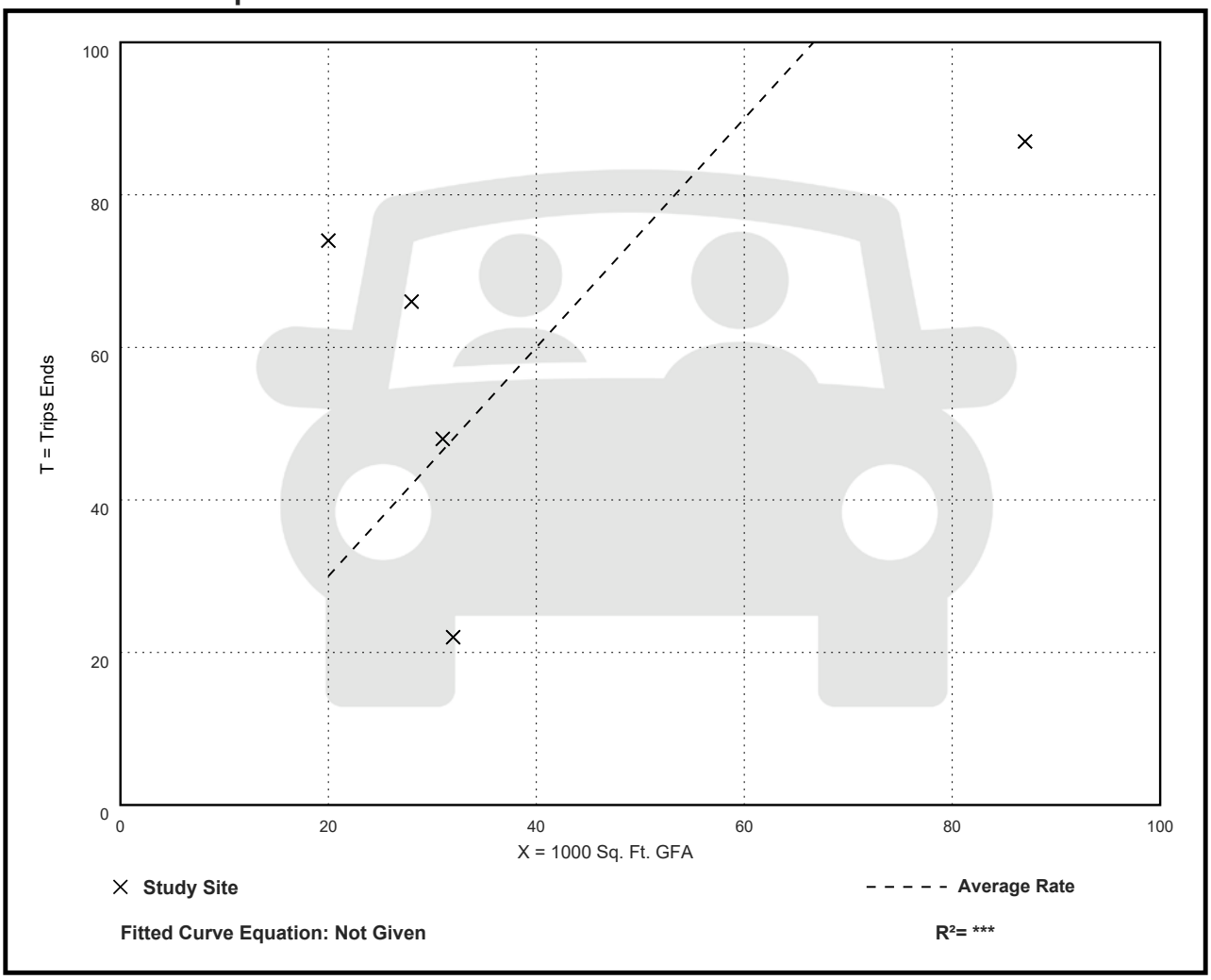
Vehicle Trip Ends vs: 1000 Sq. Ft. GFA
On a: Sunday

Setting/Location: General Urban/Suburban
Number of Studies: 5
Avg. 1000 Sq. Ft. GFA: 40
Directional Distribution: 50% entering, 50% exiting

Vehicle Trip Generation per 1000 Sq. Ft. GFA

Average Rate	Range of Rates	Standard Deviation
1.50	0.69 - 3.70	1.01

Data Plot and Equation



Attachment: 148 Mason Avenue Trip Generation (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

Mini-Warehouse
(151)

Vehicle Trip Ends vs: 1000 Sq. Ft. GFA
On a: Sunday, Peak Hour of Generator

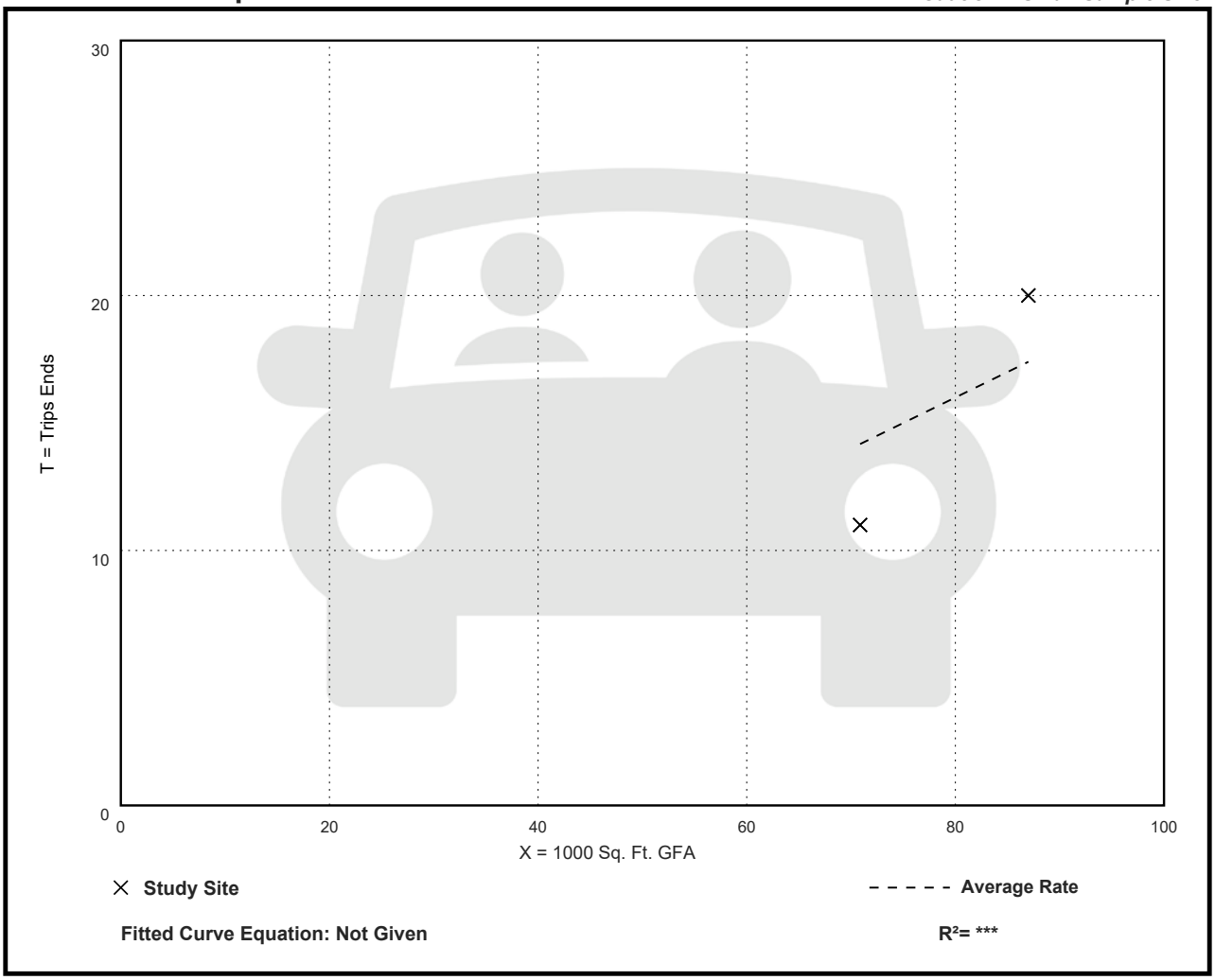
Setting/Location: General Urban/Suburban
Number of Studies: 2
Avg. 1000 Sq. Ft. GFA: 79
Directional Distribution: 45% entering, 55% exiting

Vehicle Trip Generation per 1000 Sq. Ft. GFA

Average Rate	Range of Rates	Standard Deviation
0.20	0.16 - 0.23	***

Data Plot and Equation

Caution – Small Sample Size



Attachment: 148 Mason Avenue Trip Generation (2024-O-3079 : Mason Avenue Storage Facility Planned Development)





ECS Florida, LLC

Geotechnical Engineering Report

TSS - Holly Hill

148 Mason Avenue
Holly Hill, Florida

ECS Project Number 56:1868

April 30, 2024

Attachment: Geotechnical Report (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

ECS FLORIDA, LLC
"One Firm. One Mission."
Geotechnical • Construction Materials • Environmental • Facilities

April 30, 2024

Mr. Jake French
Stein Investment Group
5607 Glenridge Drive, Suite 200
Atlanta, Georgia 30342

ECS Project No. 56:1868

Reference: Geotechnical Engineering Report
TSS - Holly Hill
148 Mason Avenue
Holly Hill, Florida

Dear Mr. French:

ECS Florida, LLC. (ECS) has completed the subsurface exploration, laboratory testing, and geotechnical engineering analyses for the above-referenced project. Our services were performed in general accordance with our agreed-to scope of work. This report presents our understanding of the geotechnical aspects of the project along with the results of the field exploration and laboratory testing conducted, and our foundation design and earthwork construction recommendations.

It has been our pleasure to be of service to **Stein Investment Group** during the design phase of this project. We would appreciate the opportunity to remain involved during the continuation of the design phase, and we would like to provide our services during construction phase operations as well to verify the assumptions of subsurface conditions made for this report. Should you have any questions concerning the information contained in this report, or if we can be of further assistance to you, please contact us.

Respectfully submitted,

ECS Florida, LLC

David W. Spangler, State of Florida
Professional Engineer, License No. 58770

This item has been digitally signed and sealed by David W. Spangler on the date indicated here.

Printed Copies of this document are not considered signed and sealed and the signature must be verified on any electronic copies.

2024.04.30 11:01:43 -04'00'

Melkin Fructuoso, EI
Geotechnical Project Manager
MFructuoso@esclimited.com

David Spangler, P.E.
Chief Engineer
Registered Florida No 58770
DSpangler@ecslimited.com

Attachment: Geotechnical Report (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

TABLE OF CONTENTS

EXECUTIVE SUMMARY **1**
1.0 INTRODUCTION **3**
2.0 PROJECT INFORMATION **4**
2.1 PROJECT LOCATION/CURRENT SITE USE 4
2.2 PAST SITE HISTORY/USES 4
2.3 SOIL SURVEY MAPPING 4
2.4 PROPOSED CONSTRUCTION 5
3.0 FIELD EXPLORATION AND LABORATORY TESTING **6**
3.1 SUBSURFACE CHARACTERIZATION 6
3.2 GROUNDWATER OBSERVATIONS 7
3.2.1 Encountered Groundwater 7
3.2.2 Estimated Normal Seasonal High Groundwater 7
3.3 LABORATORY TESTING 7
4.0 DESIGN RECOMMENDATIONS **8**
4.1 FOUNDATIONS 8
4.2 SLABS ON GRADE 9
4.3 PAVEMENTS 9
4.3.1 Flexible Pavement Recommendations 9
4.3.2 Rigid Pavement Recommendations 10
4.4 STORMWATER MANAGEMENT POND 10
4.4.1 Soil Permeability Rates 10
4.4.2 Pond Excavation Borrow Suitability 11
5.0 SITE CONSTRUCTION RECOMMENDATIONS **11**
5.1 SUBGRADE PREPARATION 11
5.1.1 Stripping and Grubbing 11
5.1.2 Over-Excavation of Organic Soils 11
5.1.3 Proof Rolling 12
5.1.4 Temporary Groundwater Control 12
5.1.5 Subgrade Compaction 12
5.2 EARTHWORK OPERATIONS 13
5.2.1 Structural Backfill and Fill Soils 13
5.2.2 Foundation Areas 14
5.2.3 Flexible Pavement Areas 14
5.2.4 Rigid Pavement Areas 14
5.3 UTILITY INSTALLATIONS 14
6.0 CLOSING **15**

Attachment: Geotechnical Report (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

APPENDICES

Appendix A – Drawings & Reports

- Figure 1 – Site Location Diagram
- Figure 2 – Boring Location Diagram
- Figure 3 – Boring Location Diagram with Provided Site Plan
- Generalized Subsurface Profiles

Appendix B – Field Operations

- Reference Notes for Boring Logs
- Subsurface Exploration Procedure: Standard Penetration Testing (SPT) ASTM D1586
- Subsurface Exploration Procedure: Hand Auger Boring ASTM D1452
- Geotechnical SPT Boring Logs
- Hand Auger Logs

Appendix C – Laboratory Test Results

- Laboratory Testing Summary

Attachment: Geotechnical Report (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

EXECUTIVE SUMMARY

This Executive Summary is intended as a very brief overview of the primary geotechnical conditions that are expected to affect design and construction of the proposed TSS - Holly Hill to be located at 148 Mason Avenue in Holly Hill, Florida. The proposed development consists of presumed three-story storage building with an approximate footprint of 32,500 square feet, proposed parking and entrance drives, and proposed stormwater management areas. Information gleaned from the Executive Summary should not be utilized in lieu of reading the entire geotechnical report. In summary, we assess the geotechnical conditions at the site to be as follows:

- Based on the results of our exploration, we consider the subsurface conditions at the site adaptable for support of the proposed structures on properly designed conventional shallow foundation systems with a maximum allowable net bearing pressure of 2,500 psf and 3,000 psf, for footings at embedment depths of 18 inches (wall footings) and 24 inches (column footings), respectively. Provided the site preparation and earthwork construction recommendations outlined in Section 5.0 of this report are performed, the parameters presented in Section 4.1 of this report may be used for foundation design.

- We consider the subsurface conditions at the site adaptable for support of flexible and rigid pavement sections when constructed on properly prepared subgrade soils as outlined in Section 5.0 of this report.

- Loose to very soils were encountered generally within the upper 4 to 6 feet of the soils during this exploration. Earthwork operations during the preparation of the building pad area and excavations of foundations will require continuous observation of yielding areas and a contingency should be included in the budget for isolated undercutting during proof roll operations. After completing the clearing and stripping operations and installing the temporary groundwater control measures (if required), the exposed surface should be compacted with a heavy vibratory roller a minimum static, at-drum weight, on the order of 8 tons to 10 tons. Dynamic cone penetrometer (DCP) soundings, performed by hand, should also be performed subsequent to the surface soil heavy compaction operations in the area of the building to confirm densification of the very loose soils within the upper 6 feet of the proposed finish floor elevation.

- At the Boring A-03 location, silty fine sand with many organic materials (designated SM/PT) was encountered within a depth range of approximately 3 to 5 feet below the ground surface. These are soils or materials potentially having or having greater than 8 percent organic materials by dry weight. Typically, we recommend complete removal of soils with many organic materials (greater than 8 percent) if encountered within structure or pavement areas of the site. Test pits are recommended at the location of Boring A-03 to determine the nature and vertical and lateral extent of soils with many organic materials, to determine if removal will be required, and the extent of such removals. Test pits should be performed under the oversight of the geotechnical engineer or the construction materials testing engineer of record for the project.

- The borings encountered groundwater at depths varying from 3.5 to 6.0 feet below the existing ground surface at the time of our exploration, with the normal seasonal high groundwater level (SHGWL) estimated from 2.5 to 5.0 feet below the ground surface; as shown on the boring logs in Appendix B. Temporary groundwater control will be necessary to compact subgrade soils where subgrade is within 2 feet of the groundwater level at the time of compaction.

Attachment: Geotechnical Report (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

- The fine sands (SP) and fine sands with silt (SP-SM) encountered at the stormwater pond locations and throughout the site can be used as structural fill. Silty and clayey fine sand (SM/SC) soils may also be used as structural fill where it is determined that these soils contain less than 20 percent fines. Silty and clayey fine sand soils with more than 20 percent fines are not recommended for use as structural fill but may be used as fill in non-structural areas.

- We recommend that ECS be provided the opportunity to review the foundation plans and earthwork specifications to verify that our recommendations have been properly interpreted and implemented. ECS should also be retained to perform the construction material testing and observations required for this project, to verify that our recommendations have been satisfied.

Attachment: Geotechnical Report (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

1.0 INTRODUCTION

The purpose of this study was to provide geotechnical information for the design of foundations, pavements and stormwater management (ponds) for the proposed TSS - Holly Hill to be located at 148 Mason Avenue in Holly Hill, Florida. The proposed development consists of a three-story storage building with an approximate footprint of 32,500 square feet, proposed parking and entrance drives, and proposed stormwater management areas.

Our services were provided in general accordance with the scope of services outlined in our Proposal No. 56:2181, dated March 19, 2024, which includes our Terms and Conditions of Service, as authorized on March 29, 2024.

This report includes the following items:

- A brief discussion of our understanding of the planned construction and imposed loading conditions.
- A presentation of the field and laboratory test procedures used, and the data obtained.
- A presentation of the existing on-site conditions, such as topography, surface vegetation, etc. as they relate to the planned construction.
- A presentation of the encountered subsurface conditions, including subsurface profiles and measured groundwater levels, estimated normal seasonal high groundwater levels, and estimated geotechnical engineering properties (as necessary).
- A geotechnical engineering evaluation of the site and subsurface conditions with respect to the planned construction.
- Recommendations for foundation design parameters, including our estimate of the performance of the foundation system.
- Recommendations for on-site flexible and rigid pavement design.
- Recommendations for the proposed stormwater management pond construction, including the results of laboratory falling head permeability testing (measured mean permeability and estimated horizontal and vertical permeability rates, Km, Kh and Kv, respectively).
- Recommendations for site clearing, subgrade preparation and fill placement / earthwork requirements.
- Recommendations for additional testing and/or consultation that might be required to complete the geotechnical assessment and related engineering for this project.

Attachment: Geotechnical Report (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

2.0 PROJECT INFORMATION

2.1 PROJECT LOCATION/CURRENT SITE USE

The project site is located at 148 Mason Avenue in Holly Hill, Florida. The site was bordered to the north by 1st Street followed by a vacant lot and single-family residential development, to the west by Daytona Avenue followed by a gas station and single-family residential development, to the east by Shirley Heyman Park including a pond followed by N Beach Street, and to the south by Mason Avenue followed by single-family residential development. A figure showing the general site location is provided below, and on Figure 1 in Appendix A.



Site Location

At the time of our exploration, the site was developed with a transmission shop with associated paved parking and drives to the east and covered of grass and some trees to the west. ECS was not provided a site topographic survey at the time of this report. Based on topographic information from the USGS Topographic Map of the site area, the estimated site elevations ranged between approximately El. 4 to El. 12. These elevation estimates are approximate and are not based on a site-specific survey; they should not be used in project design.

2.2 PAST SITE HISTORY/USES

ECS has reviewed aerial photographs of the subject site on Google Earth and Historic Aerials (NETR Online). The aerial photographs reviewed were dated 1985, 1995, 1999, 2004 to 201, 2014 to 2019 and 2021 to 2023. From 1985 to 1995, aerial photographs showed the site consisted of some trees and a transmission shop with associated parking and paved driveways, and surrounded by single-family homes. In 1995, aerial photograph showed a detention pond to the east of the site. In 2010 aerial photograph showed a cleared and leveled vacant lot to the north of the site. Site conditions did not appear to change significantly since 2010, and conditions appeared to be approximately as they existed at the time of this exploration.

2.3 SOIL SURVEY MAPPING

Based on the Web Soil Survey for Volusia County, Florida, as prepared by the U.S. Department of Agriculture Natural Resource Conservation Service (USDA-NRCS), the predominant soil type existing

Attachment: Geotechnical Report (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

within the site area and beyond the site boundaries is described in the following table. The site area is illustrated superimposed on the USDA-NRCS Soil Survey Map included as the following figure.

Web Soil Survey Data

Soil Type	Constituents	Drainage Class	Water Table
6—Astatula-Urban land complex, 0 to 8 percent slopes	Fine and	Excessively drained	More than 80 inches
71—Urban land, 0 to 2 percent slopes	N/A	N/A	N/A

Soil mapping of the site vicinity including soil type and number are presented in the following figure, obtained from the USDA Web Soil site.



Site Soil Survey

2.4 PROPOSED CONSTRUCTION

Based on email correspondence with Mr. Jake French at Stein Investment Group and the provided Concept Plan Site dated March 25, 2024, we understand that a proposed storage building development is proposed at 148 Mason Avenue in Holly Hill, Florida. The proposed development consists of presumed three-story storage building with an approximate footprint of 32,500 square feet, proposed parking and entrance drives, and proposed stormwater management areas. Details of the building construction were not provided at the time of this report. We assume that building construction will comprise masonry and wood-frame construction with a concrete slab-on-grade lower floor. Based on our experience with similar projects, maximum wall and column loads are expected to not exceed 10 kips per linear foot and 200 kips, respectively. Based on the provided information, the wet pond located to the east of the site is proposed to be expanded to the west.

Attachment: Geotechnical Report (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

3.0 FIELD EXPLORATION AND LABORATORY TESTING

Our scope of exploration work included drilling six (6) Standard Penetration Test (SPT) Borings to a depth of 25 feet below the ground surface for the proposed commercial building, two (2) SPT Borings to a depth of 15 feet below the ground surface for the proposed stormwater management (pond), and three (3) SPT Borings to a depth of 6 feet below the ground surface for the proposed pavement areas for parking and drives. Our borings were located with a handheld GPS unit and their approximate locations are shown on the Boring Location Diagram (Figures 2 and 3) in Appendix A. Our exploration procedures are explained in greater detail in Appendix B, including the inserts titled Reference Notes for Boring Logs and Subsurface Exploration Procedure: Standard Penetration Testing (SPT) ASTM D1586.

3.1 SUBSURFACE CHARACTERIZATION

The subsurface conditions encountered were generally consistent with published geological mapping. The following sections provide generalized characterizations of the soil strata. Please refer to the boring logs in Appendix B for detailed subsurface conditions.

Subsurface Stratigraphy of Building SPT Borings

Approximate Depth Range (ft)	Stratum	Description	Ranges of SPT[(1)] N-values (bpf)
0 to 0.58	N/A	Topsoil [6.00”] **As an exception, Asphalt concrete and Limerock Base, were encountered at the Boring B-05 location, approximately within the depth range of 1 to 6 inches, respectively, below the ground surface.**	N/A
0.5 to 25 [(2)]	I	Very Loose to Dense Fine Sand (SP) and Fine Sand with Silt (SP-SM), some to significant Shells.	2-42

Notes: (1) Standard Penetration Test
(2) Termination depth of borings

Subsurface Stratigraphy of Pond SPT Borings

Approximate Depth Range (ft)	Stratum	Description	Ranges of SPT[(1)] N-values (bpf)
0 to 0.5	N/A	Topsoil [6.00”]	N/A
0.5 to 15 [(2)]	I	Loose to Medium Dense Fine Sand (SP) and Fine Sand with Silt (SP-SM).	6-16

Notes: (1) Standard Penetration Test
(2) Termination depth of borings

Attachment: Geotechnical Report (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

Subsurface Stratigraphy of Pavement Auger Borings

Approximate Depth Range (ft)	Stratum	Description
0 to 0.5	N/A	Topsoil [6.00"]
0.5 to 6 (1)	I	Fine Sand (SP), Fine Sand with Silty (SP-SM) and Silty Fine Sand (SM) **As an exception, Silty Fine Sand (SM/PT) with many organic materials (greater than 8%), was encountered at the Boring A-03 location, approximately within the depth range of 3 to 5 feet below the ground surface.**

Notes: (1) Termination depth of borings

3.2 GROUNDWATER OBSERVATIONS

3.2.1 Encountered Groundwater

Groundwater levels were measured during our field exploration and are presented in our boring logs in Appendix B. Groundwater depths estimated at the time of drilling were approximately 3.5 to 6.0 feet below the ground surface. Variations in the long-term water table may occur as a result of changes in precipitation, evaporation, surface water runoff, construction activities, and other factors.

3.2.2 Estimated Normal Seasonal High Groundwater

The normal seasonal high groundwater level is affected by a number of factors. The drainage characteristics of the soils, land surface elevation, relief points such as drainage ditches, lakes, rivers, swamp areas, etc., and distance to relief points are some of the more important factors influencing the seasonal high groundwater level.

Based on the estimated groundwater levels at the site and our interpretation of the site conditions, including the boring logs and Web Soil Survey, we estimate the normal seasonal high groundwater level (SHGWL) to be approximately 1.0 foot higher than the levels estimated at the time of drilling; approximately at 2.5 to 5.0 feet below the ground surface, as shown on the attached Boring Logs. It is possible that groundwater levels may exceed the estimated normal seasonal high groundwater level as a result of significant or prolonged rains.

3.3 LABORATORY TESTING

Each sample was visually classified on the basis of texture and plasticity in accordance with ASTM D2487 Standard Practice for Classification for Engineering Purposes (Unified Soil Classification System (USCS)) and ASTM D2488 Standard Practice for Description and Identification of Soils (Visual-Manual Procedures) and including USCS classification symbols. After classification, the samples were grouped in the major zones noted on the boring logs in Appendix B. The group symbols for each soil type are indicated in parentheses along with the soil descriptions. The stratification lines between strata on the logs are approximate; in situ, the transitions may be gradual.

The laboratory testing consisted of selected tests performed on samples obtained during our field exploration. Classification and index property tests were performed on representative soil samples and included percent fines (ASTM D1140), moisture content (ASTM D2216), organic material

Attachment: Geotechnical Report (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

content (ASTM D2974), and falling head permeability (ASTM D5084) tests. Percent fines and moisture content test results are included on the boring logs in Appendix B; all laboratory tests, except the permeability test, are also summarized in Appendix C on the Laboratory Testing Summary sheet. The permeability test results are presented in Section 4.4.

4.0 DESIGN RECOMMENDATIONS

4.1 FOUNDATIONS

The recommendations presented in this report are based on the project information provided to us, the results of the soil test borings, laboratory testing, and the engineering analyses. Considering the results of our field exploration and our experience with similar projects, it is our professional opinion the existing on-site sandy soils at the project site are considered to be suitable for the proposed development, provided that the subgrade soils have been properly prepared, as described in this report, and approved by the Geotechnical Engineer or their authorized representative.

Very loose to loose sandy soils were encountered in the upper 4 to 6 feet below the existing ground surface at several boring locations within the proposed building footprint. A heavy vibratory roller should be used to compact the surface soils in the area of the building footprints. Dynamic cone penetrometer (DCP) soundings, performed by hand, should also be performed subsequent to the surface soil heavy compaction operations to confirm densification of the very loose soils within the upper 6 feet of the finished floor elevations.

Provided subgrades and structural fills are prepared as recommended in this report, the proposed structures can be supported by shallow foundations including column footings and continuous wall footings. We recommend the foundation design use the following parameters:

Buildings Foundation Parameters

Design Parameter	Column Footing	Wall Footing
Minimum Width	24 inches	18 inches
Minimum Footing Embedment Depth (below slab or finished grade)	24 inches	18 inches
Estimated Maximum Total Settlement[1]	1 inch	1 inch
Estimated Maximum Differential Settlement[2]	½ inch between columns	Less than ½ inch over 50 feet
Net Allowable Bearing Pressure[3]	2,500 psf at 18 inches embedment 3,000 psf at 24 inches embedment	
Acceptable Bearing Soil Material	Compacted Subgrade/Engineered Fill	

1. Based on estimated structural loads. If final loads are different, ECS must be contacted to update foundation recommendations and settlement calculations.
2. Based on maximum column/wall loads and variability in borings. Differential settlement can be re-evaluated once the foundation plans are more complete.
3. Net allowable bearing pressure is the applied pressure in excess of the surrounding overburden soils above the base of the foundation.

Depending on the final floor elevations of the buildings, we anticipate that the soils at the foundation bearing elevation are anticipated to be adaptable for support of the proposed structures, after subgrade preparation in accordance with Section 5.0 of this report. The bearing level soils, after compaction, should exhibit densities equivalent to 95 percent of the modified

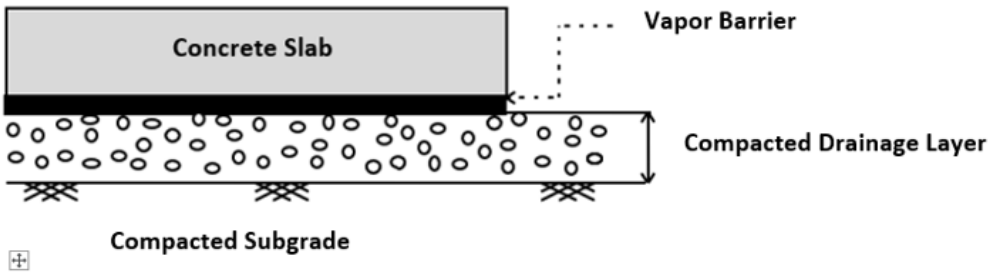
Attachment: Geotechnical Report (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

Proctor maximum dry density (ASTM D1557) to a depth of at least one foot below foundation bearing levels.

For turn down slabs and interior wall footings the minimum width should also be 18 inches, however the sloped transition portion of the turn-down may be included when determining the footing width. Even though the maximum allowable soil bearing pressure may not be achieved, these width recommendations should control the size of the foundations.

4.2 SLABS ON GRADE

The floor slabs can be constructed as a slab-on-ground, provided the site is prepared as outlined in Section 5.0. A minimum clearance of 2 feet is recommended between the estimated normal SHGWL and the bottom of the floor slabs. It is recommended the floor slab bearing soils be covered with an impervious membrane to reduce moisture entry and floor dampness. A 6-mil thick plastic membrane is commonly used for this purpose. Care should be exercised not to tear large sections of the membrane during placement of reinforcing steel and concrete. Due to the potential for a damp slab condition to develop as a result of the shallow groundwater, we recommend a minimum of 6 inches of drainage material directly beneath the floor slab and plastic membrane, as shown in Figure 4.2.1; note that this material may consist of the on-site fine sand (SP) soils or other approved imported fill. Consideration should also be given to not use moisture sensitive floor coverings.



1. Drainage Layer Thickness – 6 inches minimum
2. Drainage Layer Material – SAND (SP, SW), GRAVEL (GP, GW)

Figure 4.2.1. Granular Capillary Break/Drainage Layer

4.3 PAVEMENTS

Based on the results of our exploration, we consider the subsurface conditions at the site adaptable for support of a flexible or rigid pavement section when constructed on properly prepared subgrade soils as outlined in Section 5.0 of this report. Typical pavement sections used in northeast Florida are presented in the following sections. If requested, we can prepare a project-specific pavement design if specific traffic data is provided.

4.3.1 Flexible Pavement Recommendations

TYPICAL FLEXIBLE PAVEMENT SECTIONS		
MATERIAL	**LIGHT DUTY**	**HEAVY DUTY**
Asphaltic Concrete Surface Course (SP-9.5 or Type S)	1.5 inches	2 inches
Limerock Base	6 inches	8 inches
Stabilized Subgrade	12 inches	12 inches

Attachment: Geotechnical Report (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

Base and Subgrade: The limerock base course should have a minimum Limerock Bearing Ratio (LBR) of 100 and should be compacted to 98 percent of the modified Proctor maximum dry density (ASTM D1557) value. The subgrade material should have a minimum LBR of 40 and be compacted to 98 percent of the modified Proctor maximum dry density (ASTM D1557) value.

Underdrains: Satisfactory pavement life is dependent on dry/strong pavement support provided by the base and subgrade courses. Accordingly, a minimum clearance of 2 feet must be maintained between the normal SHGWL and the bottom of the limerock base layer. In some areas of the site, elevating fill will be required to achieve this separation. Depending on final pavement grades, FDOT Type I or II underdrains may be required to maintain dry base and subgrade materials where this separation cannot be achieved.

4.3.2 Rigid Pavement Recommendations

Our recommendations for slab thickness for standard duty and heavy-duty concrete pavements are based on the following:

a) subgrade soils densified to 98 percent of the modified Proctor maximum dry density (ASTM D1557),

b) modulus of subgrade reaction (k) equal to 200 pounds per cubic inch, and

c) a 20-year design life.

TYPICAL RIGID PAVEMENT SECTIONS		
	LIGHT DUTY	**HEAVY DUTY**
Minimum Concrete Thickness	5 inches	6 inches
Maximum Control Joint Spacing	10 feet x 10 feet	12 feet x 12 feet
Recommended Sawcut Depth	1¼ inches	1½ inches

We recommend using concrete with a minimum 28-day compressive strength of 4,000 psi and a minimum 28-day flexural strength (modulus of rupture) of at least 600 pounds per square inch, based on 3rd point loading of concrete beam test samples. Layout of the sawcut control joints should form square panels. The joints should be sawed within six hours of concrete placement or as soon as the concrete has developed sufficient strength to support workers and equipment. We recommend allowing ECS to review and comment on the final concrete pavement design, including section and joint details (type of joints, joint spacing, etc.), prior to the start of construction.

For further details on concrete pavement construction, please reference the "Guide to Jointing on Non-Reinforced Concrete Pavements" published by the Florida Concrete and Products Associates, Inc., and "Building Quality Concrete Parking Areas", published by the Portland Cement Association.

4.4 STORMWATER MANAGEMENT POND

4.4.1 Soil Permeability Rates

For the stormwater management pond, laboratory testing included soil permeability tests on remolded samples collected at the time of drilling from Boring P-01 and P-02, and the results of these tests are presented in the following table.

Attachment: Geotechnical Report (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

Laboratory Permeability Results

Test Location	Test Depth (feet)	Soil Type	Measured Mean Permeability (ft/day) K_m	Estimated Horizontal Permeability (ft/day) K_h	Estimated Vertical Permeability (ft/day) K_v
P-01	4 to 6	SP-SM	1.3	1.3	1.3
P-02	4 to 6	SP-SM	3.5	3.5	3.5

The measured permeability rates presented from the field and laboratory tests should not be construed to represent the actual pond exfiltration rates. For pond design calculations, we recommend an appropriate factor of safety be applied to the above permeability values; typically a factor of safety of 2.0 is recommended.

4.4.2 Pond Excavation Borrow Suitability

Based on the boring results and classification of the soil samples, the fine sands (SP) and fine sands with silt (SP-SM) encountered at the stormwater pond locations can be used as structural fill. If soils to be excavated from within the proposed pond areas are in close proximity to or below the groundwater level, they may have moisture contents in excess of the modified Proctor optimum moisture content. In this case, these soils will require stockpiling or spreading to drain the excess moisture. Wet soils should be dried to bring the soil moisture content within ±2 percent of the soil's optimum moisture content to facilitate placement and compaction. Dewatering also may be used to drain the soils excess moisture in advance of borrow pond area excavation; however, this would lower the water level within the existing wet pond. Clayey fine sand (SC) soils may also be used as structural fill where it is determined that these soils contain less than 20 percent fines. Clayey fine sand soils with more than 20 percent fines are not recommended for use as structural fill but may be used as fill in non-structural areas.

5.0 SITE CONSTRUCTION RECOMMENDATIONS

5.1 SUBGRADE PREPARATION

5.1.1 Stripping and Grubbing

The existing structures and structural debris, including subsurface foundations and abandoned utilities and pavements should be completely removed from the site. The "footprint" of the proposed buildings, plus a minimum additional margin of 5 feet, and of the hardscape areas (parking/driveway) plus a minimum additional margin of 3 feet, should be stripped of all existing surface vegetation, stumps, organic topsoil, or other deleterious materials (including structural debris). During grubbing operations, roots with a diameter greater than 0.5-inch, stumps, small roots in a concentrated state or other organic soils with higher than 8 percent organic materials content, should be grubbed and completely removed; organic soils may be used in non-structural areas.

5.1.2 Over-Excavation of Organic Soils

At the Boring A-03 location, silty fine sand with many organic materials (designated SM/PT) were encountered within a depth range of approximately 3 to 5 feet below the ground surface. These are soils or materials potentially having or having greater than 8 percent organic materials by dry weight. Typically, we recommend complete removal of soils with many organic materials (greater than 8 percent) if encountered within structure or pavement areas of the site. Test pits are

Attachment: Geotechnical Report (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

recommended at the location of Boring A-03 to determine the nature and vertical and lateral extent of soils with many organic materials, to determine if removal will be required, and the extent of such removals. Test pits should be performed under the oversight of the geotechnical engineer or the construction materials testing engineer of record for the project.

5.1.3 Proof Rolling

Following removal of any unsuitable materials and prior to fill placement or other construction on subgrades, subgrades should be evaluated by an ECS field technician by proof rolling. The exposed subgrade should be thoroughly proof rolled with construction equipment having a minimum axle load of 20 tons [e.g., fully loaded tandem-axle dump truck]. Proof rolling should be traversed in two perpendicular directions with overlapping passes of the vehicle under the observation of an ECS technician. This procedure is intended to assist in identifying any localized yielding materials.

Where proof rolling identifies areas that are unstable or "pumping" subgrade those areas should be repaired prior to the placement of any subsequent Structural Fill or other construction materials. Methods of stabilization include undercutting or moisture conditioning. The situation should be discussed with ECS to determine the appropriate procedure. Test pits may be excavated to explore the shallow subsurface materials to help in determining the cause of the observed unstable materials, and to assist in the evaluation of appropriate remedial actions to stabilize the subgrade.

5.1.4 Temporary Groundwater Control

We recommend that temporary groundwater control measures be implemented where the groundwater table is within a depth of 2 feet below the excavated subgrade bottom at the time of compaction operations. Dewatering methods should be determined by the contractor. We recommend the groundwater control measures remain in place until compaction of the existing soils is completed. The dewatering method should be maintained until backfilling has reached a height of 2 feet above the subgrade level at the time of construction. The site should be graded to direct surface water runoff from the construction area.

Note that discharge of produced groundwater to surface waters of the state from dewatering operations or other site activities is regulated and requires a permit from the State of Florida Department of Environmental Protection (FDEP). This permit is termed a Generic Permit for the Discharge of Produced Groundwater From Any Non-Contaminated Site Activity. If discharge of produced groundwater is anticipated, we recommend sampling and testing of the groundwater early in the site design phase to prevent project delays during construction. ECS can provide the sampling, testing, and professional consulting required to evaluate compliance with the regulations.

5.1.5 Subgrade Compaction

After completing the clearing and stripping, installing the temporary groundwater control measures, unsuitable (organic or other) materials removals (where required) and proof rolling operations, the exposed surface should be compacted with a heavy vibratory roller having a minimum static, at-drum weight on the order of 10 tons to compact disturbed or very loose to loose soils near subgrade levels. Typically, the material should exhibit moisture contents within ±2 percentage points of the modified Proctor optimum moisture content (ASTM D1557) during the compaction operations. Compaction should continue until densities of at least 95 percent of the modified Proctor maximum dry density (ASTM D1557) have been achieved within the upper 2 feet of the compacted natural soils at the site. Dynamic cone penetrometer (DCP) soundings, performed by hand, should also be performed subsequent to the surface soil heavy compaction operations in

Attachment: Geotechnical Report (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

the area of the building to confirm densification of the very loose soils within the upper 6 feet of the proposed finish floor elevation.

Should the bearing level soils experience pumping and soil strength loss during the compaction operations, compaction work should be immediately terminated, and (1) the disturbed soils should be removed and backfilled with compacted structural fill, or (2) the excess moisture content within the disturbed soils should be allowed to dissipate before recompacting.

Care should be exercised to avoid damaging any nearby structures while the compaction operation is underway. Prior to commencing compaction, occupants of adjacent structures should be notified, and the existing conditions of the structures should be documented with photographs and survey (if deemed necessary). Compaction should cease if deemed detrimental to adjacent structures, and ECS should be contacted immediately. We recommend the vibratory roller remain a minimum of 50 feet from existing structures. Within this zone, use of a track-mounted bulldozer, or a vibratory roller operating in the static mode, is recommended.

5.2 EARTHWORK OPERATIONS

5.2.1 Structural Backfill and Fill Soils

Structural fill is defined as a non-plastic, inorganic, granular soil having less than 10 percent material passing the No. 200 mesh sieve and containing less than 4 percent organic material. The predominant fine sands and fine sands with silt (SP, SP-SM), as encountered in the borings, may be used as structural fill materials and, with proper moisture control, should densify using conventional compaction methods. Soils with more than 10 to 12 percent passing the No. 200 sieve will be more difficult to compact, due to their nature to retain soil moisture, and may require drying. The clayey fine sand (SC) (and silty fine sand (SM) if encountered) in some borings may be used as structural fill where it is determined that these soils contain 20 percent or less fines; however, the potential difficulty working with these soils and achieving optimum moisture content for earthwork should be taken into consideration. Soils with more than 20 percent fines are not recommended for use as structural fill.

Structural Fill Compaction Requirements: Materials placed as structural fill should meet the following compaction requirements.

STRUCTURAL FILL COMPACTION REQUIREMENTS	
Subject	**Requirement**
Compaction Standard	Modified Proctor, ASTM D1557
Required Compaction	95% of Max. Dry Density (general structural fill) 98% of Max. Dry Density (upper one foot below the proposed pavement base course)
Loose Thickness prior to compaction	12 inches if vibratory drum roller compaction equipment is used 8 inches if vibratory drum roller is used in static mode 8 inches if track-mounted compaction equipment is used 6 inches if hand-held compaction equipment is used

Fill materials should not be placed on excessively wet soils. Excessively wet soils should be scarified, aerated, and moisture conditioned. Proper drainage should be maintained during the earthwork phases of construction to prevent ponding of water which has a tendency to degrade subgrade soils. The contractor should minimize dusting or implement dust control measures, as required.

Attachment: Geotechnical Report (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

We recommend that the grading contractor have equipment on site during earthwork for both drying and wetting fill soils. Moisture control may be difficult during extended periods of rain. The control of moisture content of soils containing more than 10% fines may be difficult when these soils become wet. Further, such soils are easily degraded by construction traffic when the moisture content is elevated.

5.2.2 Foundation Areas

After satisfactory placement and compaction of the required structural fill, the foundation areas may be excavated to the planned bearing levels. The foundation bearing level soils, after compaction, should exhibit densities equivalent to 95 percent of the modified Proctor maximum dry density (ASTM D1557) to a depth of at least one foot below the bearing level. For confined areas, such as the footing excavations, any compactive effort should be provided by a lightweight vibratory sled or roller having a total weight on the order of 500 to 2,000 pounds.

5.2.3 Flexible Pavement Areas

After completing the clearing/stripping operations in the pavement areas, where any underlying clayey (or silty) sands with more than 20 percent fines are determined to be within 2 feet of the bottom of the pavement base, they should be over-excavated from within the pavement areas and should be replaced with approved on-site or imported structural fill. Structural backfill and fill required to achieve the finish pavement grades then can be placed and compacted as described in Sections 5.2.1.

5.2.4 Rigid Pavement Areas

For a concrete pavement subgrade, we recommend using clean fine sand (SP), compacted to at least 98 percent of modified Proctor test maximum dry density (ASTM D1557) without additional stabilization. Limerock base is not required beneath rigid pavements and the relatively free draining fine sand (SP) soils with 5 percent or less fines are preferred.

5.3 UTILITY INSTALLATIONS

Utility Subgrades: The soil borings encountered predominant fine sands and fine sands with silt (SP, SP-SM), and may encounter clayey fine sand (SC), or silty fine sand (SM) in some areas of the site. It is our opinion that these soils are suitable bedding soils for pipelines and utility structures where it is determined that these soils contain 20 percent or less fines. Where soils contain more than 20 percent fines, they should be over excavated to a depth of 12 inches below the pipe invert and to a depth of 24 inches below manhole structures, and should be replaced with soils having less than 20 percent fines.

Utility Backfilling: Backfill placed around the pipe, and to a height of 2 feet above the top of pipe, should be placed in 6-inch lifts. Each lift should be compacted with hand-held equipment to 98 percent of the soil's Modified Proctor (ASTM D1557) maximum dry density. Backfill placed above the 2-foot zone above the top of pipe elevation may be placed in 12-inch lifts and compacted with heavier equipment. Typically, the backfill soil should exhibit moisture contents within ±2 percent of the soil's optimum moisture content as determined from the Proctor test. Care should be taken to avoid damaging the pipe during compaction operations.

Utility Excavation Dewatering: Based on the groundwater depths encountered at our boring locations, groundwater may be encountered in utility excavations which extend below existing grades. Removal of groundwater may be required, especially for deeper utility excavations. The contractor should submit a dewatering plan prior to installing the site utilities.

Attachment: Geotechnical Report (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

Excavation Safety: All excavations and slopes should be made and maintained in accordance with OSHA excavation safety standards. The contractor is solely responsible for designing and constructing stable, temporary excavations and slopes and should shore, slope, or bench the sides of the excavations and slopes as required to maintain stability of both the excavation sides and bottom. The contractor's responsible person, as defined in 29 CFR Part 1926, should evaluate the soil exposed in the excavations as part of the contractor's safety procedures. In no case should slope height, slope inclination, or excavation depth, including utility trench excavation depth, exceed those specified in local, state, and federal safety regulations. ECS is providing this information solely as a service to our client. ECS is not assuming responsibility for construction site safety or the contractor's activities; such responsibility is not being implied and should not be inferred.

Erosion Control: The surface soils may be erodible. Therefore, the Contractor should provide and maintain good site drainage during earthwork operations to maintain the integrity of the surface soils. All erosion and sedimentation controls should be in accordance with sound engineering practices and local requirements.

Other Excavation Considerations: Dense to very dense coquina gravel and/or cemented shells were encountered throughout many of the borings at this site. Excavations through this material may be difficult and require special equipment or procedures, particularly where the near-surface materials are cemented.

6.0 CLOSING

Our geotechnical exploration has been performed, our findings obtained, and our recommendations prepared, in accordance with generally accepted geotechnical engineering principles and practices. ECS is not responsible for any independent conclusions, interpretation, opinions, or recommendations made by others based on the data contained in this report.

Our scope of services was intended to evaluate the soil conditions within the zone of soil influenced by the foundation and pavement systems. Our scope of services does not address geologic conditions, such as sinkholes or soil conditions existing below the depth of the soil borings.

If any of the project description information discussed in this report is inaccurate, either due to our interpretation of the documents provided or site or design changes that may occur later, ECS should be contacted immediately in order that we can review the report in light of the changes and provide additional or alternate recommendations as may be required to reflect the proposed construction.

We recommend that ECS be allowed to review the project's plans and specifications pertaining to our work so that we may ascertain consistency of those plans/specifications with the intent of the geotechnical report.

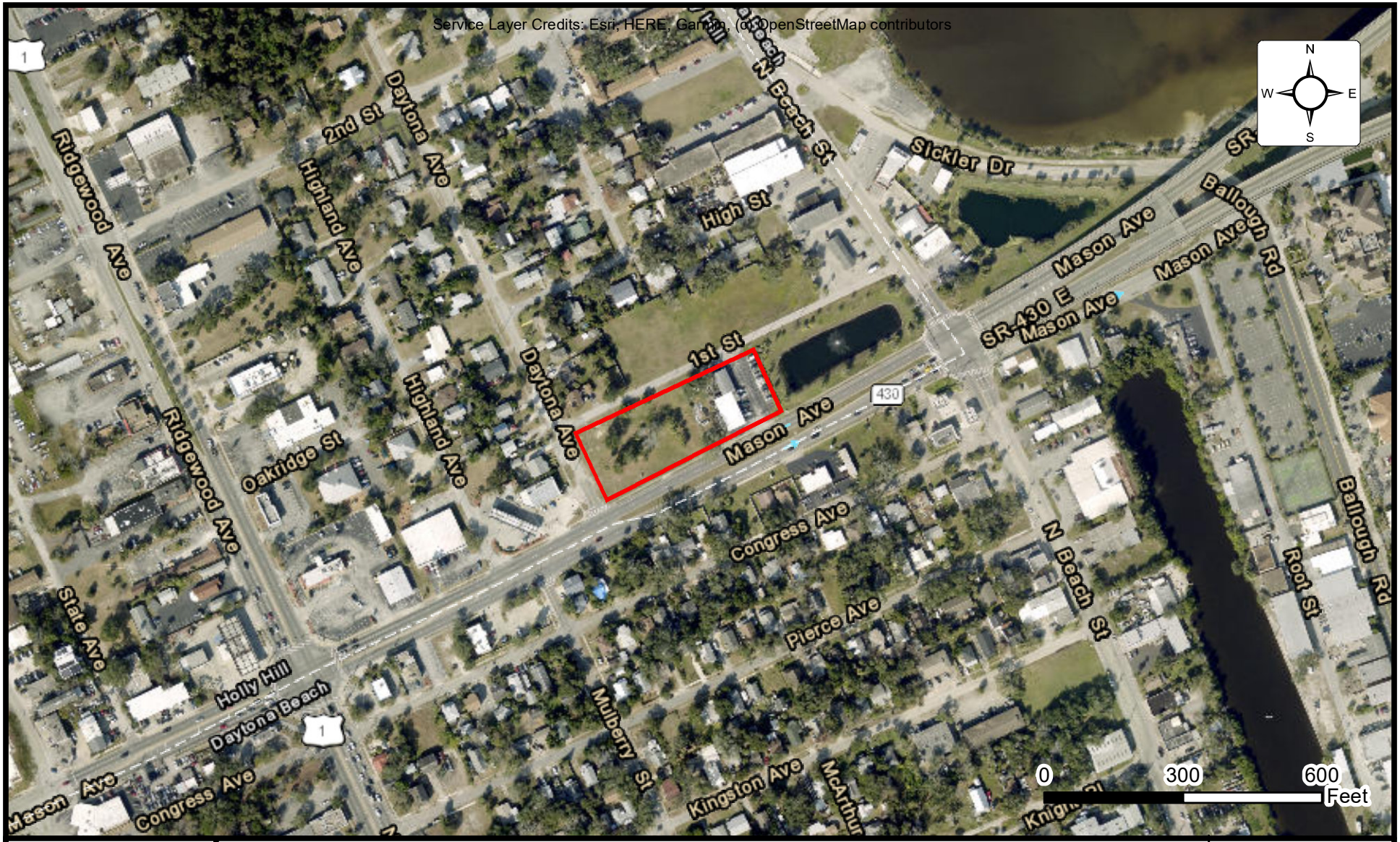
Field observations, monitoring, and quality assurance testing during earthwork and foundation installation are an extension of and integral to the geotechnical design recommendation. We recommend that the owner retain these quality assurance services and that ECS be allowed to continue our involvement throughout these critical phases of construction to provide general consultation as issues arise.

Attachment: Geotechnical Report (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

APPENDIX A – Diagrams & Reports

Figure 1 – Site Location Diagram
Figure 2 – Boring Location Diagram
Figure 3 – Boring Location Diagram with Provided Site Plan
Subsurface Soil Profiles

Attachment: Geotechnical Report (2024-O-3079 : Mason Avenue Storage Facility Planned Development)



SITE LOCATION DIAGRAM
TSS - HOLLY HILL

148 MASON AVENUE, HOLLY HILL, FLORIDA
STEIN INVESTMENT GROUP

ENGINEER	MK6
SCALE	AS NOTED
PROJECT NO.	56:1868
FIGURE	1 OF 3
DATE	4/25/2024

Attachment: Geotechnical Report (2024-O-3079 : Mason Avenue Storage Facility Planned Development)



BORING LOCATION DIAGRAM
TSS - HOLLY HILL

148 MASON AVENUE, HOLLY HILL, FLORIDA
STEIN INVESTMENT GROUP

ENGINEER	MK6
SCALE	AS NOTED
PROJECT NO.	56:1868
FIGURE	2 OF 3
DATE	4/30/2024

Attachment: Geotechnical Report (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

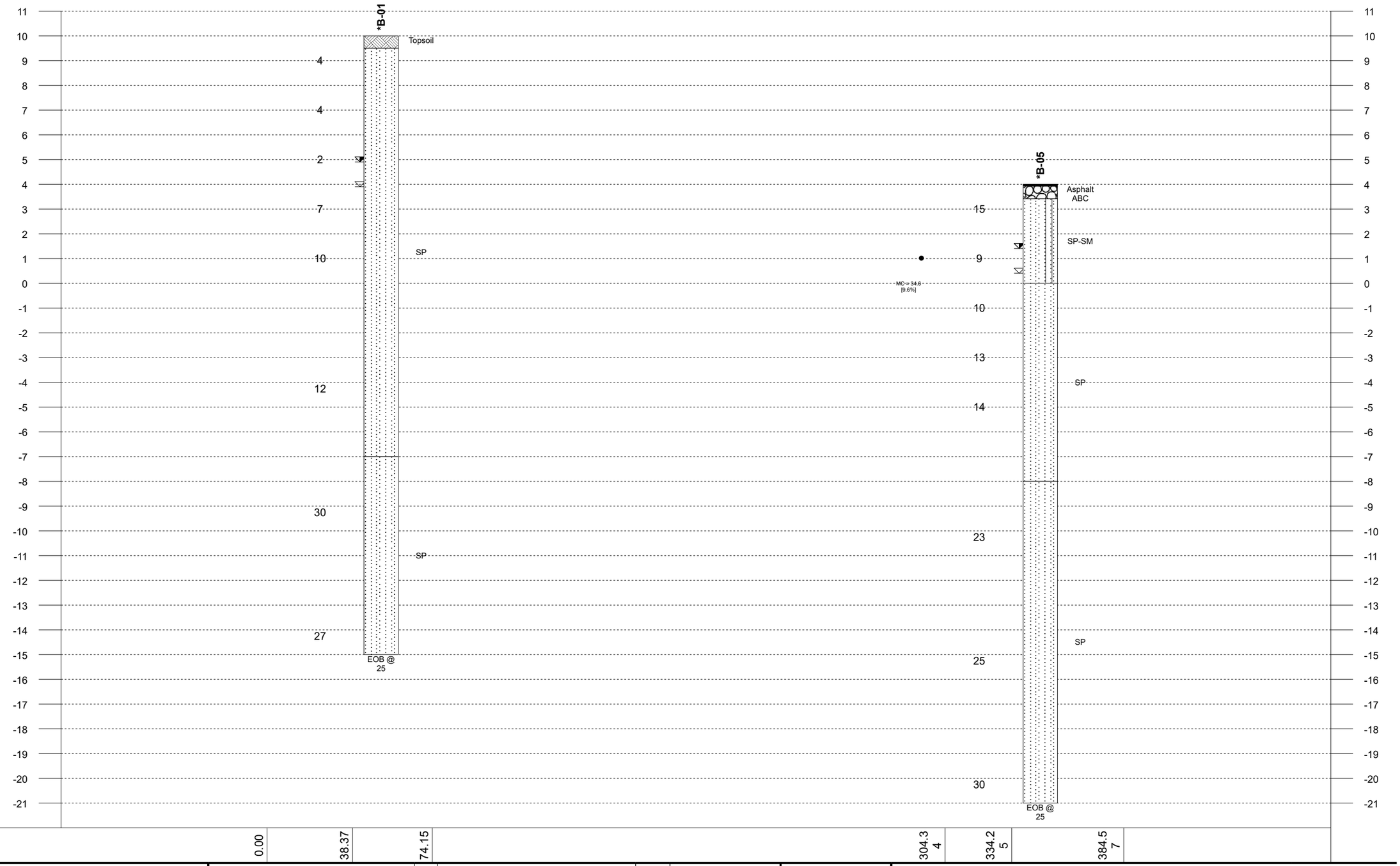


BORING LOCATION DIAGRAM
TSS - HOLLY HILL

148 MASON AVENUE, HOLLY HILL, FLORIDA
STEIN INVESTMENT GROUP

ENGINEER	MK6
SCALE	AS NOTED
PROJECT NO.	56:1868
FIGURE	3 OF 3
DATE	4/30/2024

Attachment: Geotechnical Report (2024-O-3079 : Mason Avenue Storage Facility Planned Development)



Notes:

1- EOB: END OF BORING AR: AUGER REFUSAL SR: SAMPLER REFUSAL.
2- THE NUMBER BELOW THE STRIPS IS THE DISTANCE ALONG THE BASELINE.
3- SEE INDIVIDUAL BORING LOG AND GEOTECHNICAL INFORMATION.
4- STANDARD PENETRATION TEST RESISTANCE (LEFT OF BORING) IN BLOWS PER FOOT (ASTM D1586).

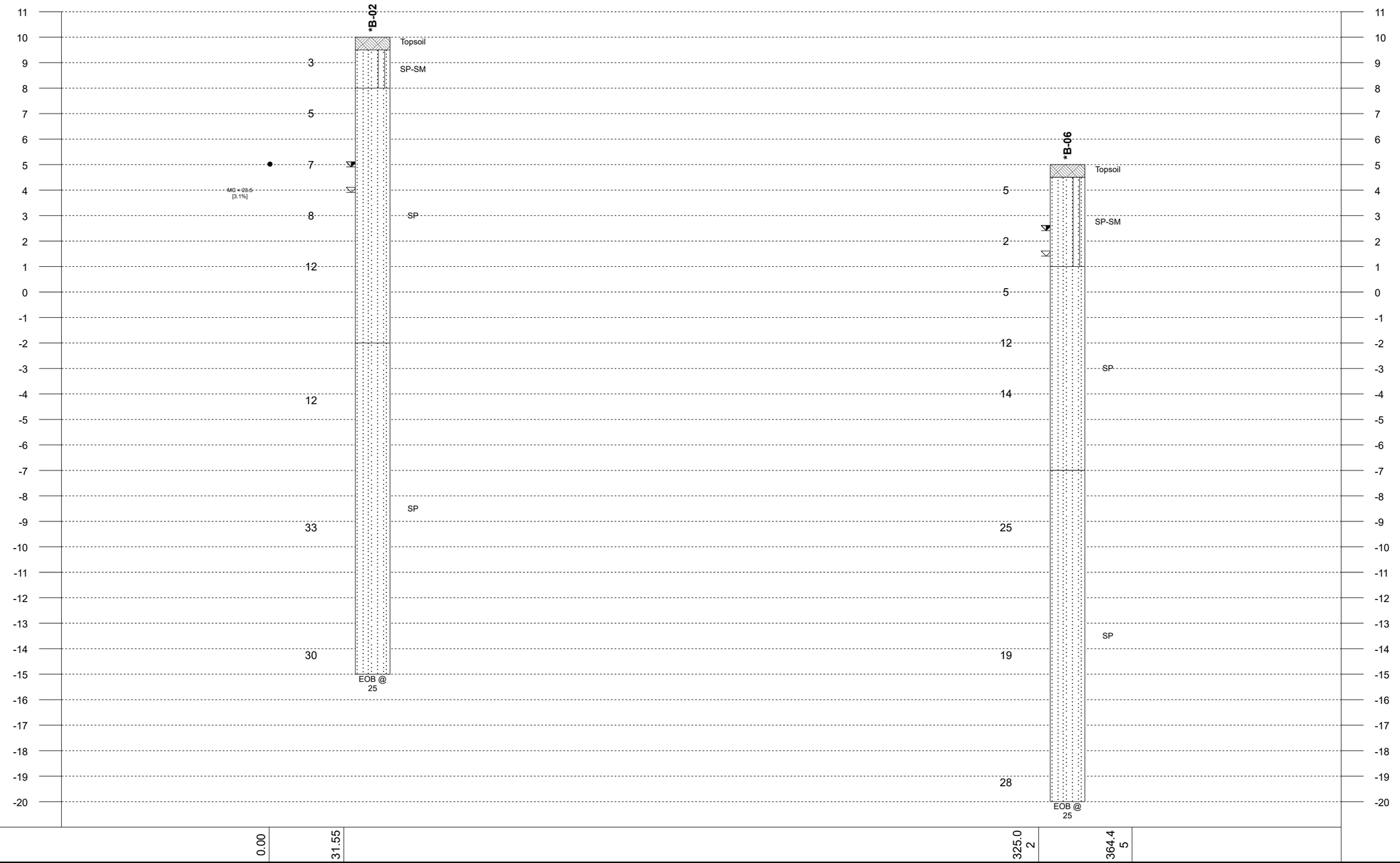
Plastic Limit Water Content Liquid Limit X—●—△	WL (First Encountered)	Fill
[FINES CONTENT%]	WL (Completion)	Possible Fill
BOTTOM OF CASING	WL (Seasonal High Water)	Probable Fill
LOSS OF CIRCULATION	WL (Stabilized)	Rock

GENERALIZED SUBSURFACE PROFILE Section line A-A'

TSS - Holly Hill
Stein Investment Group
148 Mason Avenue, Holly Hill, Florida, 32117

Project No: 56:1868 Date:

Attachment: Geotechnical Report (2024-O-3079 : Mason Avenue Storage Facility Planned Development)



Legend Key

- Topsoil
- SP-SM
- SP
- -21.00

Notes:

1- EOB: END OF BORING AR: AUGER REFUSAL SR: SAMPLER REFUSAL.
2- THE NUMBER BELOW THE STRIPS IS THE DISTANCE ALONG THE BASELINE.
3- SEE INDIVIDUAL BORING LOG AND GEOTECHNICAL INFORMATION.
4- STANDARD PENETRATION TEST RESISTANCE (LEFT OF BORING) IN BLOWS PER FOOT (ASTM D1586).

Plastic Limit Water Content Liquid Limit
[FINES CONTENT%]
BOTTOM OF CASING
LOSS OF CIRCULATION

WL (First Encountered)
WL (Completion)
WL (Seasonal High Water)
WL (Stabilized)

Fill
Possible Fill
Probable Fill
Rock

GENERALIZED SUBSURFACE PROFILE Section line B-B'

TSS - Holly Hill
Stein Investment Group
148 Mason Avenue, Holly Hill, Florida, 32117

Project No: 56:1868 Date:

Attachment: Geotechnical Report (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

APPENDIX B – Field Operations

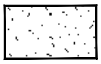
Reference Notes for Boring Logs
Subsurface Exploration Procedure: Standard Penetration Testing (SPT) ASTM D1586
Subsurface Exploration Procedure: Hand Auger Boring ASTM D1452
Geotechnical SPT Boring Logs
Hand Auger Logs

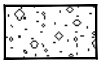
Attachment: Geotechnical Report (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

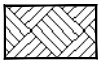
REFERENCE NOTES FOR BORING LOGS

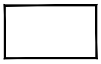
MATERIAL[1,2]

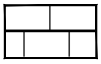

ASPHALT


CONCRETE


GRAVEL

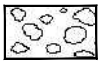

TOPSOIL

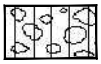

VOID


BRICK

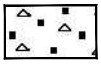

AGGREGATE BASE COURSE

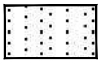

GW **WELL-GRADED GRAVEL**
gravel-sand mixtures, little or no fines

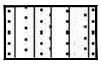

GP **POORLY-GRADED GRAVEL**
gravel-sand mixtures, little or no fines


GM **SILTY GRAVEL**
gravel-sand-silt mixtures

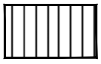

GC **CLAYEY GRAVEL**
gravel-sand-clay mixtures

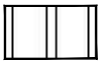

SW **WELL-GRADED SAND**
gravelly sand, little or no fines

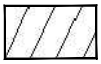

SP **POORLY-GRADED SAND**
gravelly sand, little or no fines


SM **SILTY SAND**
sand-silt mixtures

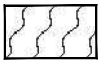

SC **CLAYEY SAND**
sand-clay mixtures

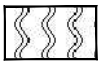

ML **SILT**
non-plastic to medium plasticity

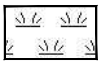

MH **ELASTIC SILT**
high plasticity


CL **LEAN CLAY**
low to medium plasticity


CH **FAT CLAY**
high plasticity


OL **ORGANIC SILT or CLAY**
non-plastic to low plasticity


OH **ORGANIC SILT or CLAY**
high plasticity


PT **PEAT**
highly organic soils

DRILLING SAMPLING SYMBOLS & ABBREVIATIONS

SS	Split Spoon Sampler	PM	Pressuremeter Test
ST	Shelby Tube Sampler	RD	Rock Bit Drilling
WS	Wash Sample	RC	Rock Core, NX, BX, AX
BS	Bulk Sample of Cuttings	REC	Rock Sample Recovery %
PA	Power Auger (no sample)	RQD	Rock Quality Designation %
HSA	Hollow Stem Auger		

PARTICLE SIZE IDENTIFICATION

DESIGNATION		PARTICLE SIZES
Boulders		12 inches (300 mm) or larger
Cobbles		3 inches to 12 inches (75 mm to 300 mm)
Gravel:	Coarse	¾ inch to 3 inches (19 mm to 75 mm)
	Fine	4.75 mm to 19 mm (No. 4 sieve to ¾ inch)
Sand:	Coarse	2.00 mm to 4.75 mm (No. 10 to No. 4 sieve)
	Medium	0.425 mm to 2.00 mm (No. 40 to No. 10 sieve)
	Fine	0.074 mm to 0.425 mm (No. 200 to No. 40 sieve)
Silt & Clay ("Fines")		<0.074 mm (smaller than a No. 200 sieve)

COHESIVE SILTS & CLAYS

UNCONFINED COMPRESSIVE STRENGTH, Q_P[4]	SPT[5] (BPF)	CONSISTENCY[7] (COHESIVE)
<0.25	<2	Very Soft
0.25 - <0.50	2 - 4	Soft
0.50 - <1.00	5 - 8	Firm
1.00 - <2.00	9 - 15	Stiff
2.00 - <4.00	16 - 30	Very Stiff
4.00 - 8.00	31 - 50	Hard
>8.00	>50	Very Hard

GRAVELS, SANDS & NON-COHESIVE SILTS

SPT[5]	DENSITY
<5	Very Loose
5 - 10	Loose
11 - 30	Medium Dense
31 - 50	Dense
>50	Very Dense

RELATIVE AMOUNT[7]	COARSE GRAINED (%)[8]	FINE GRAINED (%)[8]
Trace	≤5	≤5
With	10 - 20	10 - 25
Adjective *(ex: "Silty")*	25 - 45	30 - 45

WATER LEVELS[6]

- WL (First Encountered)
- WL (Completion)
- WL (Seasonal High Water)
- WL (Stabilized)

FILL AND ROCK

FILL | POSSIBLE FILL | PROBABLE FILL | ROCK

[1]Classifications and symbols per ASTM D 2488-17 (Visual-Manual Procedure) unless noted otherwise.

[2]To be consistent with general practice, "POORLY GRADED" has been removed from GP, GP-GM, GP-GC, SP, SP-SM, SP-SC soil types on the boring logs.

[3]Non-ASTM designations are included in soil descriptions and symbols along with ASTM symbol [Ex: (SM-FILL)].

[4]Typically estimated via pocket penetrometer or Torvane shear test and expressed in tons per square foot (tsf).

[5]Standard Penetration Test (SPT) refers to the number of hammer blows (blow count) of a 140 lb. hammer falling 30 inches on a 2 inch OD split spoon sampler required to drive the sampler 12 inches (ASTM D 1586). "N-value" is another term for "blow count" and is expressed in blows per foot (bpf). SPT correlations per 7.4.2 Method B and need to be corrected if using an auto hammer.

[6]The water levels are those levels actually measured in the borehole at the times indicated by the symbol. The measurements are relatively reliable when augering, without adding fluids, in granular soils. In clay and cohesive silts, the determination of water levels may require several days for the water level to stabilize. In such cases, additional methods of measurement are generally employed.

[7]Minor deviation from ASTM D 2488-17 Note 14.

[8]Percentages are estimated to the nearest 5% per ASTM D 2488-17.

Attachment: Geotechnical Report (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

© 2021 ECS Corporate Services, LLC.

SUBSURFACE EXPLORATION PROCEDURE: STANDARD PENETRATION TESTING (SPT) ASTM D 1586 Split-Barrel Sampling

Standard Penetration Testing, or **SPT**, is the most frequently used subsurface exploration test performed worldwide. This test provides samples for identification purposes, as well as a measure of penetration resistance, or N-value. The N-Value, or blow counts, when corrected and correlated, can approximate engineering properties of soils used for geotechnical design and engineering purposes.

SPT Procedure:

- Involves driving a hollow tube (split-spoon) into the ground by dropping a 140-lb hammer a height of 30-inches at desired depth
- Recording the number of hammer blows required to drive split-spoon a distance of 12 inches (in 3 or 4 Increments of 6 inches each)



- Auger is advanced* and an additional SPT is performed
- One SPT test is typically performed for every two to five feet



- Obtain 1.5-inch diameter soil sample

**Drilling Methods May Vary—* The predominant drilling methods used for SPT are open hole fluid rotary drilling and hollow-stem auger drilling.

Attachment: Geotechnical Report (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

SUBSURFACE EXPLORATION PROCEDURE: SOIL EXPLORATION AND SAMPLING BY AUGER BORINGS

ASTM D 1452

The auger borings were performed manually by the use of a hand auger and in general accordance with the latest revision of ASTM D 1452, “Soil Investigation and Sampling by Auger Borings”. Representative samples of the soils brought to the ground surface by the augering process were placed in sealed containers and transported to our laboratory where they were examined by our engineer to verify the driller’s field classification.

HAND AUGER BORING:





Attachment: Geotechnical Report (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

CLIENT:	PROJECT NO.:	SHEET:
Stein Investment Group	**56:1868**	**1 of 1**
PROJECT NAME:	HAND AUGER NO.:	SURFACE ELEVATION:
TSS - Holly Hill	**A-01**	**8.0**
SITE LOCATION:		STATION:
148 Mason Avenue, Holly Hill, Florida, 32117		
LATITUDE: **29.228024**	LONGITUDE: **-81.029178**	

DEPTH (FT)	WATER LEVELS	ELEVATION (FT)	DESCRIPTION OF MATERIAL	EXCAVATION EFFORT	DCP	SAMPLE NUMBER	FINES CONTENT (%)	MOISTURE CONTENT (%)
			Topsoil Thickness[6.00"]			S-1		
			(SP) FINE SAND, gray, brown and orange, moist			S-2		
5	▽ ▼	3				S-3		
			END OF HAND AUGER AT 6 FT					
10		-2						
15								

REMARKS:

THE STRATIFICATION LINES REPRESENT THE APPROXIMATE BOUNDRY LINES BETWEEN SOIL TYPES. IN-SITU THE TRANSITION MAY BE GRADUAL

EXCAVATION EFFORT: E - EASY M - MEDIUM D - DIFFICULT VD - VERY DIFFICULT

▽ WL (First Encountered) **6.00**	▼ WL (Seasonal High) **5.00**	ECS REP:	DATE COMPLETED:	UNITS:	CAVE-IN-DEPTH
▼ WL (Completion)			**Apr 11 2024**	**English**	

HAND AUGER LOG

Attachment: Geotechnical Report (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

CLIENT:	PROJECT NO.:	SHEET:
Stein Investment Group	**56:1868**	**1 of 1**
PROJECT NAME:	HAND AUGER NO.:	SURFACE ELEVATION:
TSS - Holly Hill	**A-02**	**5.0**
SITE LOCATION:		STATION:
148 Mason Avenue, Holly Hill, Florida, 32117		
LATITUDE: **29.228291**	LONGITUDE: **-81.028523**	

DEPTH (FT)	WATER LEVELS	ELEVATION (FT)	DESCRIPTION OF MATERIAL	EXCAVATION EFFORT	DCP	SAMPLE NUMBER	FINES CONTENT (%)	MOISTURE CONTENT (%)
			Topsoil Thickness[6.00"]			S-1		
			(SP) FINE SAND, gray, moist					
			(SP-SM) FINE SAND WITH SILT, brown to dark brown, moist to saturated			S-2	8	22.9
	▽							
	▼					S-3		
5		0						
			END OF HAND AUGER AT 6 FT					
10		-5						
15								

REMARKS:

THE STRATIFICATION LINES REPRESENT THE APPROXIMATE BOUNDRY LINES BETWEEN SOIL TYPES. IN-SITU THE TRANSITION MAY BE GRADUAL

EXCAVATION EFFORT: E - EASY M - MEDIUM D - DIFFICULT VD - VERY DIFFICULT

▽ WL (First Encountered) **4.00**	▼ WL (Seasonal High) **3.00**	ECS REP:	DATE COMPLETED:	UNITS:	CAVE-IN-DEPTH
▼ WL (Completion)			**Apr 11 2024**	**English**	

HAND AUGER LOG

Attachment: Geotechnical Report (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

CLIENT:	PROJECT NO.:	SHEET:
Stein Investment Group	**56:1868**	**1 of 1**
PROJECT NAME:	HAND AUGER NO.:	SURFACE ELEVATION:
TSS - Holly Hill	**A-03**	**4.0**
SITE LOCATION:		STATION:
148 Mason Avenue, Holly Hill, Florida, 32117		
LATITUDE: **29.228159**	LONGITUDE: **-81.028282**	

DEPTH (FT)	WATER LEVELS	ELEVATION (FT)	DESCRIPTION OF MATERIAL	EXCAVATION EFFORT	DCP	SAMPLE NUMBER	FINES CONTENT (%)	MOISTURE CONTENT (%)
			Topsoil Thickness[6.00"]			S-1		
			(SP-SM) FINE SAND WITH SILT, brown and orange, moist			S-2		
	▽					S-3	14	51.7
	▽		(SM/PT) SILTY FINE SAND, many organics, dark brown, moist to saturated					
5		-1	(SP-SM) FINE SAND WITH SILT, dark brown, saturated			S-4		
			END OF HAND AUGER AT 6 FT					
10		-6						
15								

REMARKS:

THE STRATIFICATION LINES REPRESENT THE APPROXIMATE BOUNDRY LINES BETWEEN SOIL TYPES. IN-SITU THE TRANSITION MAY BE GRADUAL

EXCAVATION EFFORT: E - EASY M - MEDIUM D - DIFFICULT VD - VERY DIFFICULT

▽ WL (First Encountered) **4.00**	▼ WL (Seasonal High) **3.00**	ECS REP:	DATE COMPLETED:	UNITS:	CAVE-IN-DEPTH
▼ WL (Completion)			**Apr 11 2024**	**English**	

HAND AUGER LOG

Attachment: Geotechnical Report (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

CLIENT:	PROJECT NO.:	BORING NO.:	SHEET:
Stein Investment Group	**56:1868**	**B-01**	**1 of 1**
PROJECT NAME:	DRILLER/CONTRACTOR:		
TSS - Holly Hill	**Allstate Geotechnical Drilling Inc.**		
SITE LOCATION:			LOSS OF CIRCULATION
148 Mason Avenue, Holly Hill, Florida, 32117			
LATITUDE:	LONGITUDE:	STATION:	SURFACE ELEVATION:
29.227898	**-81.029237**		**10.0**

DEPTH (FT)	SAMPLE NUMBER	SAMPLE TYPE	SAMPLE DIST. (IN)	RECOVERY (IN)	DESCRIPTION OF MATERIAL	ELEVATION (FT)	BLOWS/6" (N - Value)*
0	S-1	SS	24	24	Topsoil Thickness[6.00"]	10	2-2-2-2 (4)
					(SP) FINE SAND, brown to light brown, moist to saturated, very loose to medium dense		
	S-2	SS	24	24			2-2-2-2 (4)
5	S-3	SS	24	24		5	1-1-1-1 (2)
	S-4	SS	24	24			2-3-4-5 (7)
	S-5	SS	24	24			4-5-5-6 (10)
10						0	
15	S-6	SS	18	18		-5	2-3-9 (12)
					(SP) FINE SAND, light brown, saturated, dense, significant shells		
20	S-7	SS	18	18		-10	11-14-16 (30)
25	S-8	SS	18	18		-15	10-12-15 (27)
					END OF BORING AT 25 FT		
30						-20	

STANDARD PENETRATION BLOWS/FT
10 20 30 40 50
20 40 60 80 100
ROCK QUALITY DESIGNATION & RECOVERY
RQD
REC
MODIFIED CALIFORNIA SAMPLER BLOWS/FT
10 20 30 40 50

LIQUID LIMIT
PLASTIC LIMIT
CALIBRATED PENETROMETER TSF
1 2 3 4 5
WATER CONTENT %
[FINES CONTENT] %
10 20 30 40 50

THE STRATIFICATION LINES REPRESENT THE APPROXIMATE BOUNDARY LINES BETWEEN SOIL TYPES. IN-SITU THE TRANSITION MAY BE GRADUAL

WL (First Encountered)	**6.00**	BORING STARTED: **Apr 11 2024**	CAVE IN DEPTH:	
WL (Completion)		BORING COMPLETED: **Apr 11 2024**	HAMMER TYPE: **Auto**	
WL (Seasonal High Water)	**5.00**	EQUIPMENT: **Track**	LOGGED BY:	DRILLING METHOD:
WL (Stabilized)				

GEOTECHNICAL BOREHOLE LOG

Attachment: Geotechnical Report (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

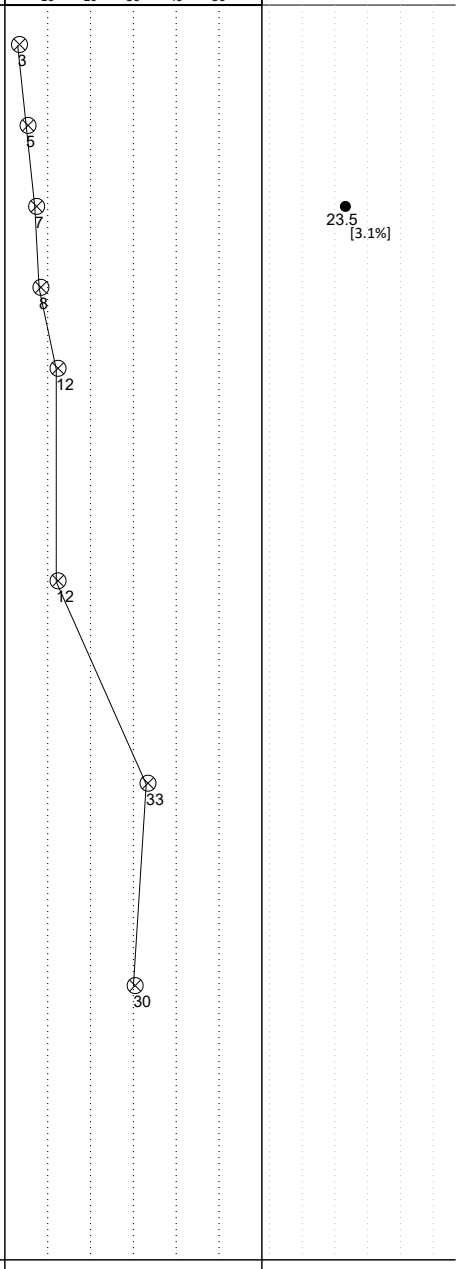
CLIENT:	PROJECT NO.:	BORING NO.:	SHEET:
Stein Investment Group	**56:1868**	**B-02**	**1 of 1**
PROJECT NAME:	DRILLER/CONTRACTOR:		
TSS - Holly Hill	**Allstate Geotechnical Drilling Inc.**		
SITE LOCATION:			LOSS OF CIRCULATION
148 Mason Avenue, Holly Hill, Florida, 32117			
LATITUDE:	LONGITUDE:	STATION:	SURFACE ELEVATION:
29.227739	**-81.029135**		**10.0**

BOTTOM OF CASING

DEPTH (FT)	SAMPLE NUMBER	SAMPLE TYPE	SAMPLE DIST. (IN)	RECOVERY (IN)	DESCRIPTION OF MATERIAL	ELEVATION (FT)	BLOWS/6" (N - Value)*
	S-1	SS	24	24	Topsoil Thickness[6.00"] (SP-SM) FINE SAND WITH SILT, contains slight roots, brown, moist, loose		1-1-2-2 (3)
	S-2	SS	24	24	(SP) FINE SAND, brown to light brown, moist to saturated, loose to medium dense		2-3-2-2 (5)
5	S-3	SS	24	24		5	3-4-3-4 (7)
	S-4	SS	24	24			4-4-4-6 (8)
	S-5	SS	24	24			4-7-5-9 (12)
10						0	
	S-6	SS	18	18	(SP) FINE SAND, light brown, saturated, medium dense to dense, significant shells		7-7-5 (12)
15						-5	
	S-7	SS	18	18			10-13-20 (33)
20						-10	
	S-8	SS	18	18			17-15-15 (30)
25					**END OF BORING AT 25 FT**	-15	
30						-20	

STANDARD PENETRATION BLOWS/FT
10 20 30 40 50
20 40 60 80 100
ROCK QUALITY DESIGNATION & RECOVERY
RQD
REC
MODIFIED CALIFORNIA SAMPLER BLOWS/FT
10 20 30 40 50

LIQUID LIMIT
PLASTIC LIMIT
CALIBRATED PENETROMETER TSF
1 2 3 4 5
WATER CONTENT %
[FINES CONTENT] %
10 20 30 40 50



THE STRATIFICATION LINES REPRESENT THE APPROXIMATE BOUNDARY LINES BETWEEN SOIL TYPES. IN-SITU THE TRANSITION MAY BE GRADUAL

▽ WL (First Encountered)	**6.00**	BORING STARTED: **Apr 11 2024**	CAVE IN DEPTH:
▼ WL (Completion)		BORING COMPLETED: **Apr 11 2024**	HAMMER TYPE: **Auto**
▼ WL (Seasonal High Water)	**5.00**	EQUIPMENT: **Track** / LOGGED BY:	DRILLING METHOD:
▽ WL (Stabilized)			

GEOTECHNICAL BOREHOLE LOG

Attachment: Geotechnical Report (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

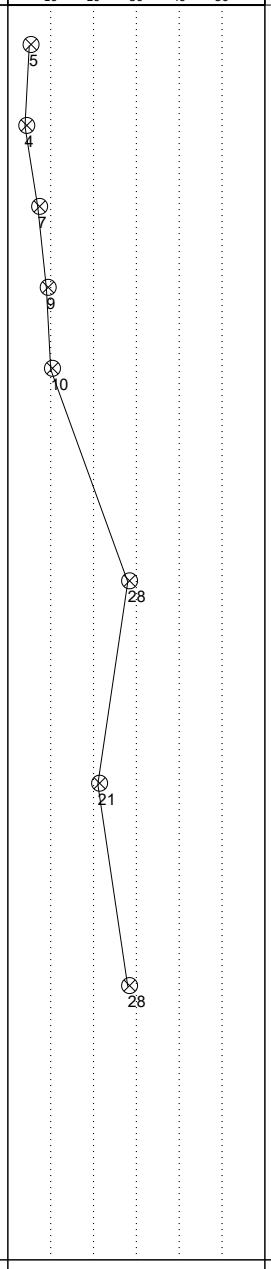
CLIENT:	PROJECT NO.:	BORING NO.:	SHEET:
Stein Investment Group	**56:1868**	**B-03**	**1 of 1**
PROJECT NAME:	DRILLER/CONTRACTOR:		
TSS - Holly Hill	**Allstate Geotechnical Drilling Inc.**		
SITE LOCATION:			LOSS OF CIRCULATION
148 Mason Avenue, Holly Hill, Florida, 32117			
LATITUDE:	LONGITUDE:	STATION:	SURFACE ELEVATION:
29.227921	**-81.028933**		**6.0**

BOTTOM OF CASING

DEPTH (FT)	SAMPLE NUMBER	SAMPLE TYPE	SAMPLE DIST. (IN)	RECOVERY (IN)	DESCRIPTION OF MATERIAL	WATER LEVELS	ELEVATION (FT)	BLOWS/6" (N - Value)*
	S-1	SS	24	24	Topsoil Thickness[6.00"] (SP) FINE SAND, brown to light brown, moist to saturated, loose to medium dense			1-2-3-4 (5)
	S-2	SS	24	24				2-2-4 (4)
5	S-3	SS	24	24			1	2-3-4-5 (7)
	S-4	SS	24	24				4-4-5-6 (9)
	S-5	SS	24	24				4-5-5-9 (10)
10							-4	
					(SP) FINE SAND, light brown, saturated, medium dense to dense, some to significant shells			
	S-6	SS	18	18				12-15-13 (28)
15							-9	
	S-7	SS	18	18				8-10-11 (21)
20							-14	
	S-8	SS	18	18				7-12-16 (28)
25					**END OF BORING AT 25 FT**		-19	
30							-24	

STANDARD PENETRATION BLOWS/FT
10 20 30 40 50
20 40 60 80 100
ROCK QUALITY DESIGNATION & RECOVERY
RQD
REC
MODIFIED CALIFORNIA SAMPLER BLOWS/FT
10 20 30 40 50

LIQUID LIMIT
PLASTIC LIMIT
CALIBRATED PENETROMETER TSF
1 2 3 4 5
WATER CONTENT %
[FINES CONTENT] %
10 20 30 40 50



THE STRATIFICATION LINES REPRESENT THE APPROXIMATE BOUNDARY LINES BETWEEN SOIL TYPES. IN-SITU THE TRANSITION MAY BE GRADUAL

▽ WL (First Encountered)	**4.00**	BORING STARTED: **Apr 11 2024**	CAVE IN DEPTH:
▼ WL (Completion)		BORING COMPLETED: **Apr 11 2024**	HAMMER TYPE: **Auto**
▼ WL (Seasonal High Water)	**3.00**	EQUIPMENT: **Track** / LOGGED BY:	DRILLING METHOD:
▽ WL (Stabilized)			

GEOTECHNICAL BOREHOLE LOG

Attachment: Geotechnical Report (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

CLIENT:	PROJECT NO.:	BORING NO.:	SHEET:
Stein Investment Group	**56:1868**	**B-04**	**1 of 1**

PROJECT NAME:	DRILLER/CONTRACTOR:
TSS - Holly Hill	**Allstate Geotechnical Drilling Inc.**

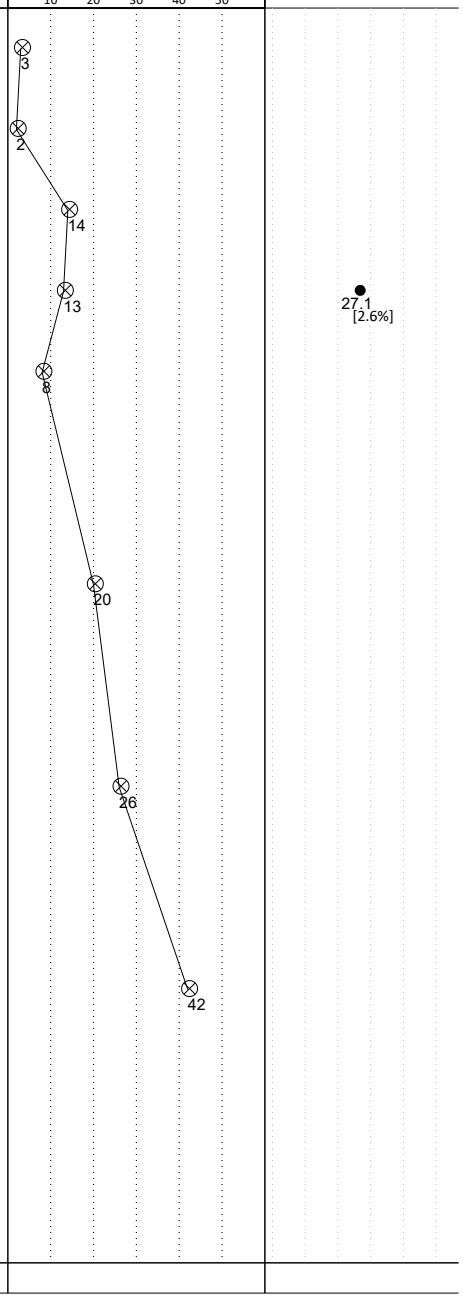
SITE LOCATION: **148 Mason Avenue, Holly Hill, Florida, 32117**

LOSS OF CIRCULATION

LATITUDE:	LONGITUDE:	STATION:	SURFACE ELEVATION:
29.228080	**-81.028537**		**6.0**

BOTTOM OF CASING

DEPTH (FT)	SAMPLE NUMBER	SAMPLE TYPE	SAMPLE DIST. (IN)	RECOVERY (IN)	DESCRIPTION OF MATERIAL	WATER LEVELS	ELEVATION (FT)	BLOWS/6" (N - Value)*
	S-1	SS	24	24	Topsoil Thickness[6.00"] (SP) FINE SAND, brown to light brown, moist, very loose			2-2-1-2 (3)
	S-2	SS	24	24	(SP-SM) FINE SAND WITH SILT, brown, moist to saturated, very loose to medium dense	▼ ▽		2-1-1-2 (2)
5	S-3	SS	24	24			1	3-5-9-11 (14)
	S-4	SS	24	24	(SP) FINE SAND, brown, saturated, loose to medium dense			5-7-6-9 (13)
	S-5	SS	24	24				4-4-4-4 (8)
10							-4	
	S-6	SS	18	18	(SP) FINE SAND, light gray, saturated, medium dense to dense, significant shells			10-12-8 (20)
15							-9	
	S-7	SS	18	18				9-14-12 (26)
20							-14	
	S-8	SS	18	18				11-16-26 (42)
25					**END OF BORING AT 25 FT**		-19	
30							-24	



THE STRATIFICATION LINES REPRESENT THE APPROXIMATE BOUNDARY LINES BETWEEN SOIL TYPES. IN-SITU THE TRANSITION MAY BE GRADUAL

▽ WL (First Encountered)	**3.50**	BORING STARTED: **Apr 11 2024**	CAVE IN DEPTH:
▼ WL (Completion)		BORING COMPLETED: **Apr 11 2024**	HAMMER TYPE: **Manual**
▼▽ WL (Seasonal High Water)	**2.50**	EQUIPMENT: **Track** / LOGGED BY:	DRILLING METHOD:
▽▽ WL (Stabilized)			

GEOTECHNICAL BOREHOLE LOG

Attachment: Geotechnical Report (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

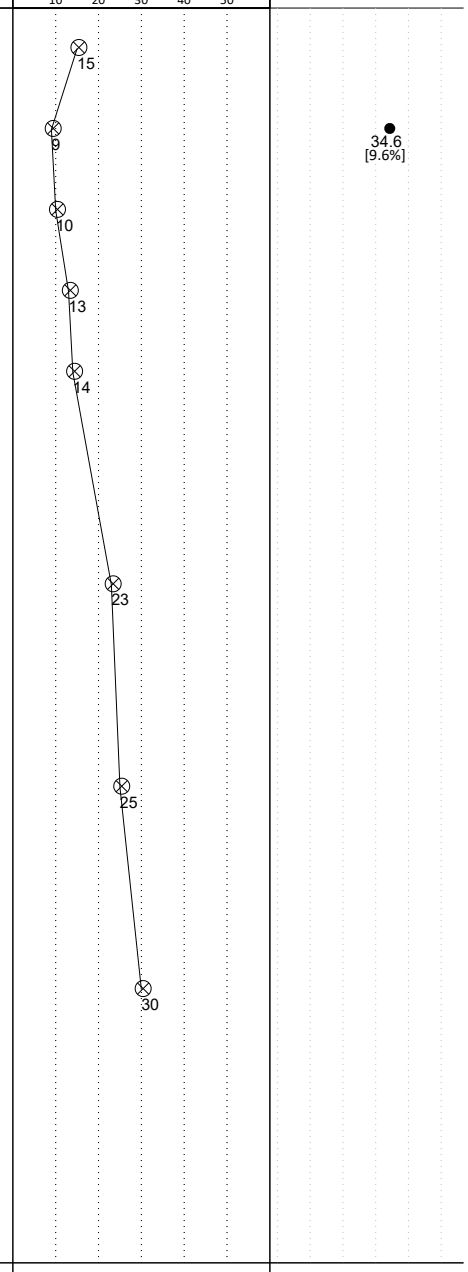
CLIENT:	PROJECT NO.:	BORING NO.:	SHEET:
Stein Investment Group	**56:1868**	**B-05**	**1 of 1**
PROJECT NAME:	DRILLER/CONTRACTOR:		
TSS - Holly Hill	**Allstate Geotechnical Drilling Inc.**		
SITE LOCATION:			LOSS OF CIRCULATION
148 Mason Avenue, Holly Hill, Florida, 32117			
LATITUDE:	LONGITUDE:	STATION:	SURFACE ELEVATION:
29.228244	**-81.028397**		**4.0**

BOTTOM OF CASING

DEPTH (FT)	SAMPLE NUMBER	SAMPLE TYPE	SAMPLE DIST. (IN)	RECOVERY (IN)	DESCRIPTION OF MATERIAL	WATER LEVELS	ELEVATION (FT)	BLOWS/6" (N - Value)*
	S-1	SS	24	24	Asphalt Thickness[1.00"] Limerock Base Thickness[6.00"] (SP-SM) FINE SAND WITH SILT, orange and dark brown, moist to saturated, loose to medium dense			6-7-8-6 (15)
	S-2	SS	24	24				6-5-4-3 (9)
5	S-3	SS	24	24	(SP) FINE SAND, brown, saturated, medium dense		-1	5-5-5-7 (10)
	S-4	SS	24	24				4-5-8-11 (13)
	S-5	SS	24	24				3-7-7-9 (14)
10							-6	
	S-6	SS	18	18	(SP) FINE SAND, light gray, saturated, medium dense to dense, significant shells			7-12-11 (23)
15							-11	
	S-7	SS	18	18				8-11-14 (25)
20							-16	
	S-8	SS	18	18				8-12-18 (30)
25					**END OF BORING AT 25 FT**		-21	
30							-26	

STANDARD PENETRATION BLOWS/FT
10 20 30 40 50
ROCK QUALITY DESIGNATION & RECOVERY
20 40 60 80 100
RQD
REC
MODIFIED CALIFORNIA SAMPLER BLOWS/FT
10 20 30 40 50

LIQUID LIMIT
PLASTIC LIMIT
CALIBRATED PENETROMETER TSF
1 2 3 4 5
WATER CONTENT %
[FINES CONTENT] %
10 20 30 40 50



THE STRATIFICATION LINES REPRESENT THE APPROXIMATE BOUNDARY LINES BETWEEN SOIL TYPES. IN-SITU THE TRANSITION MAY BE GRADUAL

▽ WL (First Encountered)	**3.50**	BORING STARTED: **Apr 11 2024**	CAVE IN DEPTH:
▼ WL (Completion)		BORING COMPLETED: **Apr 11 2024**	HAMMER TYPE: **Manual**
▼ WL (Seasonal High Water)	**2.50**	EQUIPMENT: **Track**	LOGGED BY: DRILLING METHOD:
▽ WL (Stabilized)			

GEOTECHNICAL BOREHOLE LOG

Attachment: Geotechnical Report (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

CLIENT:	PROJECT NO.:	BORING NO.:	SHEET:
Stein Investment Group	**56:1868**	**B-06**	**1 of 1**

PROJECT NAME:	DRILLER/CONTRACTOR:
TSS - Holly Hill	**Allstate Geotechnical Drilling Inc.**

SITE LOCATION: **148 Mason Avenue, Holly Hill, Florida, 32117**

LOSS OF CIRCULATION

LATITUDE:	LONGITUDE:	STATION:	SURFACE ELEVATION:	BOTTOM OF CASING
29.228069	**-81.028295**		**5.0**	

DEPTH (FT)	SAMPLE NUMBER	SAMPLE TYPE	SAMPLE DIST. (IN)	RECOVERY (IN)	DESCRIPTION OF MATERIAL	WATER LEVELS	ELEVATION (FT)	BLOWS/6" (N - Value)*
	S-1	SS	24	24	Topsoil Thickness[6.00"] (SP-SM) FINE SAND WITH SILT, contains slight roots, brown, moist to saturated, very loose to loose		5	2-2-3-2 (5)
	S-2	SS	24	24		▼ ▽	2	2-1-1-1 (2)
5	S-3	SS	24	24	(SP) FINE SAND, brown to light brown, saturated, loose to medium dense		0	2-2-3-4 (5)
	S-4	SS	24	24			5	4-5-7-8 (12)
	S-5	SS	24	24			12	5-6-8-6 (14)
10							14	
					(SP) FINE SAND, light gray, saturated, medium dense, significant shells		-5	
	S-6	SS	18	18			25	13-13-12 (25)
15							-10	
	S-7	SS	18	18			19	10-10-9 (19)
20							-15	
	S-8	SS	18	18			28	10-13-15 (28)
25					**END OF BORING AT 25 FT**		-20	
30							-25	

STANDARD PENETRATION BLOWS/FT
10 20 30 40 50
20 40 60 80 100
ROCK QUALITY DESIGNATION & RECOVERY
RQD
REC
MODIFIED CALIFORNIA SAMPLER BLOWS/FT
10 20 30 40 50

△ LIQUID LIMIT
× PLASTIC LIMIT

○ CALIBRATED PENETROMETER TSF
1 2 3 4 5

● WATER CONTENT %
[FINES CONTENT] %
10 20 30 40 50

THE STRATIFICATION LINES REPRESENT THE APPROXIMATE BOUNDARY LINES BETWEEN SOIL TYPES. IN-SITU THE TRANSITION MAY BE GRADUAL

▽ WL (First Encountered)	**3.50**	BORING STARTED: **Apr 11 2024**	CAVE IN DEPTH:
▼ WL (Completion)		BORING COMPLETED: **Apr 11 2024**	HAMMER TYPE: **Manual**
▼▽ WL (Seasonal High Water)	**2.50**	EQUIPMENT: **Track** / LOGGED BY:	DRILLING METHOD:
▽▽ WL (Stabilized)			

GEOTECHNICAL BOREHOLE LOG

Attachment: Geotechnical Report (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

CLIENT:	PROJECT NO.:	BORING NO.:	SHEET:
Stein Investment Group	**56:1868**	**P-01**	**1 of 1**

PROJECT NAME:	DRILLER/CONTRACTOR:
TSS - Holly Hill	**Allstate Geotechnical Drilling Inc.**

SITE LOCATION: **148 Mason Avenue, Holly Hill, Florida, 32117**

LOSS OF CIRCULATION

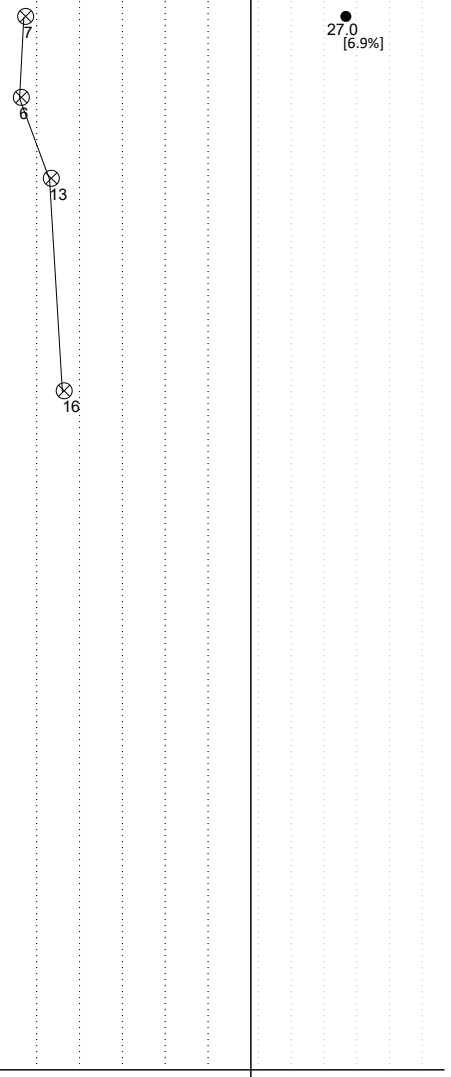
LATITUDE:	LONGITUDE:	STATION:	SURFACE ELEVATION:
29.228389	**-81.028169**		**4.0**

BOTTOM OF CASING

DEPTH (FT)	SAMPLE NUMBER	SAMPLE TYPE	SAMPLE DIST. (IN)	RECOVERY (IN)	DESCRIPTION OF MATERIAL	ELEVATION (FT)	BLOWS/6" (N - Value)*
0	S-1	SS	0	0	Topsoil Thickness[6.00"]		
					(SP-SM) FINE SAND WITH SILT, brown, moist to saturated, loose		
	S-2	SS	0	0			
5	S-3	SS	24	24		-1	4-3-4-4 (7)
	S-4	SS	24	24	(SP) FINE SAND, brown, saturated, loose to medium dense		2-3-3-4 (6)
	S-5	SS	24	24			5-5-8-15 (13)
10						-6	
	S-6	SS	18	18			6-8-8 (16)
15					**END OF BORING AT 15 FT**	-11	
20						-16	
25						-21	
30						-26	

STANDARD PENETRATION BLOWS/FT
10 20 30 40 50
20 40 60 80 100
ROCK QUALITY DESIGNATION & RECOVERY
RQD
REC
MODIFIED CALIFORNIA SAMPLER BLOWS/FT
10 20 30 40 50

LIQUID LIMIT
PLASTIC LIMIT
CALIBRATED PENETROMETER TSF
1 2 3 4 5
WATER CONTENT %
[FINES CONTENT] %
10 20 30 40 50



THE STRATIFICATION LINES REPRESENT THE APPROXIMATE BOUNDARY LINES BETWEEN SOIL TYPES. IN-SITU THE TRANSITION MAY BE GRADUAL

▽ WL (First Encountered)	**4.00**	BORING STARTED: **Apr 11 2024**	CAVE IN DEPTH:	
▼ WL (Completion)		BORING COMPLETED: **Apr 11 2024**	HAMMER TYPE: **Auto**	
▼ WL (Seasonal High Water)	**3.00**	EQUIPMENT: **Track**	LOGGED BY:	DRILLING METHOD:
▽ WL (Stabilized)				

GEOTECHNICAL BOREHOLE LOG

Attachment: Geotechnical Report (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

CLIENT:	PROJECT NO.:	BORING NO.:	SHEET:
Stein Investment Group	**56:1868**	**P-02**	**1 of 1**
PROJECT NAME:	DRILLER/CONTRACTOR:		
TSS - Holly Hill	**Allstate Geotechnical Drilling Inc.**		
SITE LOCATION:			LOSS OF CIRCULATION
148 Mason Avenue, Holly Hill, Florida, 32117			
LATITUDE:	LONGITUDE:	STATION:	SURFACE ELEVATION:
29.228221	**-81.028075**		**4.0**

BOTTOM OF CASING

DEPTH (FT)	SAMPLE NUMBER	SAMPLE TYPE	SAMPLE DIST. (IN)	RECOVERY (IN)	DESCRIPTION OF MATERIAL	WATER LEVELS	ELEVATION (FT)	BLOWS/6" (N - Value)*
	S-1	SS	0	0	Topsoil Thickness[6.00"]			
	S-2	SS	0	0	(SP-SM) FINE SAND WITH SILT AND GRAVEL, brown to dark brown, moist to saturated, medium dense	▼ ▽		
5	S-3	SS	24	24			-1	3-4-4-4 (8)
	S-4	SS	24	24	(SP) FINE SAND, brown, saturated, medium dense			4-5-5-5 (10)
	S-5	SS	24	24	(SP-SM) FINE SAND WITH SILT, brown, saturated, medium dense			6-4-5-5 (9)
10					(SP) FINE SAND, brown, saturated, medium dense		-6	
	S-6	SS	18	18				5-5-6 (11)
15					**END OF BORING AT 15 FT**		-11	
20							-16	
25							-21	
30							-26	

STANDARD PENETRATION BLOWS/FT
10 20 30 40 50
20 40 60 80 100
ROCK QUALITY DESIGNATION & RECOVERY
RQD
REC
MODIFIED CALIFORNIA SAMPLER BLOWS/FT
10 20 30 40 50

LIQUID LIMIT
PLASTIC LIMIT
CALIBRATED PENETROMETER TSF
1 2 3 4 5
WATER CONTENT %
[FINES CONTENT] %
10 20 30 40 50

8
10
9
11
28.4 [6.9%]
23.4 [5.3%]

THE STRATIFICATION LINES REPRESENT THE APPROXIMATE BOUNDARY LINES BETWEEN SOIL TYPES. IN-SITU THE TRANSITION MAY BE GRADUAL

▽ WL (First Encountered)	**4.00**	BORING STARTED: **Apr 11 2024**	CAVE IN DEPTH:
▼ WL (Completion)		BORING COMPLETED: **Apr 11 2024**	HAMMER TYPE: **Auto**
▼ WL (Seasonal High Water)	**3.00**	EQUIPMENT: **Track** / LOGGED BY:	DRILLING METHOD:
▽ WL (Stabilized)			

GEOTECHNICAL BOREHOLE LOG

Attachment: Geotechnical Report (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

APPENDIX C – Laboratory Testing

Laboratory Testing Summary

Attachment: Geotechnical Report (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

Laboratory Testing Summary

Sample Location	Sample Number	Depth (feet)	^MC (%)	Soil Type	Atterberg Limits			**Percent Passing No. 200 Sieve	Moisture - Density		@ LBR (%)	#Organic Content (%
					LL	PL	PI		<Maximum Density (pcf)	<Optimum Moisture (%)		
A-02	S-2	1.5-4	22.9	SP-SM				8.2				
A-03	S-3	3-5	51.7	SM/PT				14.0				10.3
B-02	S-3	4-6	23.5	SP				3.1				
B-04	S-4	6-8	27.1	SP				2.6				
B-05	S-2	2-4	34.6	SP-SM				9.6				
P-01	S-3	4-6	27.0	SP-SM				6.9				
P-02	S-3	4-6	28.4	SP-SM				6.9				
P-02	S-5	8-10	23.4	SP-SM				5.3				

Notes: See test reports for test method, ^ASTM D2216-19, *ASTM D2488, **ASTM D1140-17, @FM 5-515, #ASTM D2974-20e1 < See test report for D4718 corrected values

Definitions: MC: Moisture Content, Soil Type: USCS (Unified Soil Classification System), LL: Liquid Limit, PL: Plastic Limit, PI: Plasticity Index, CBR: California Bearing Ratio, OC: Organic Content

Project: TSS - Holly Hill
Client: Stein Investment Group

Project No.: 56:1868
Date Reported: 4/25/2024

Office / Lab	Address	Office Number / Fax
ECS Florida LLC - Daytona Beach	2330 South Nova Road Suite A South Daytona, FL 32119	(386)944-9588 (386)944-9589

Tested by	Checked by	Approved by	Date Received
RRawson	RRawson	RRawson	

Attachment: Geotechnical Report (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

HOLLY HILL
FLORIDA
1065 Ridgewood Avenue, Holly Hill, FL 32117
Phone: (386) 248-9442 Fax: (386) 248-9498 Permitdesk@hollyhillfl.org

01/2023

REZONE/ FUTURE LAND USE AMENDMENT

Date Received:_____ Application ID:_____ Submitted By:_____

PROJECT INFORMATION:

PROJECT NAME: 148 Mason Avenue PD
PARCEL ID #(S): see attached list of parcels
LOCATION: corner of Mason Avenue & Daytona Avenue
EXISTING USE(S): vacant commercial/commercial
PROPOSED USE(S): storage building
TOTAL ACREAGE: 1.544 +/- acres
WATER PROVIDER: _____ SEWER PROVIDER: _____
PRIVATE WELL _____ PRIVATE SEPTIC _____
CURRENT ZONING: CC-1 PROPOSED ZONING: PUD
CURRENT FUTURE LAND USE: GRC PROPOSED FUTURE LAND USE: GRC

APPLICANT INFORMATION:

Name: Mark A. Watts, Esq./Nika K. Hosseini, Esq. E-Mail: delanduse@cobbcole.com
Address: 231 N. Woodland Blvd., DeLand, FL 32720 Phone: (386) 736-7700
Company: Cobb Cole Fax: _____

☐ Owner ☒ Agent for Owner ☐ Attorney for Owner

OWNER INFORMATION:

Name: see attached list of owners E-Mail: _____
Address: _____ Phone: _____
Fax: _____

CONSULTANT INFORMATION:

Name: _____ E-Mail: _____
Address: _____ Phone: _____
Company: _____ Fax: _____

Attachment: PUD application with parcel information sheets (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

HOLLY HILL
FLORIDA
1065 Ridgewood Avenue, Holly Hill, FL 32117
Phone: (386) 248-9442 Fax: (386) 248-9498 Permitdesk@hollyhillfl.org

01/2023

WHO SHOULD ALL COMMUNICATION BE DIRECTED TO?

__X__ APPLICANT _____ OWNER _____ CONSULTANT

APPLICATION TYPE(S)/FEE(S)*

LAND USE AMENDMENT

- ☐ LARGE SCALE FUTURE LAND USE AMENDMENT (>10 ACRES) $3,000.00
- ☐ SMALL SCALE FUTURE LAND USE AMENDMENT (≤10 ACRES) $2,000.00

REZONE (NON-PD)

- ☐ STRAIGHT REZONE / LDR TEXT AMENDMENT $1,400

REZONE (PD)

- ☑ PD REZONE $2,000
- ☐ MAJOR AMENDMENT TO EXISTING PD $1,250
- ☐ MINOR AMENDMENT TO EXISTING PD $400 (This does not include changes in uses items such or density but means minor changes such as layout and landscaping that do not affect the overall intent or "spirit" of the PD.

***THERE MAY BE ADDITIONAL PASS-THROUGH FEES FOR REVIEWS DONE BY REVIEWERS OUTSIDE OF THIS AGENCY. ALL FEES ARE DUE AT THE TIME OF APPLICATION SUBMITTAL.**

ATTACHMENT CHECKLIST

REQUIRED SUBMITTALS

- ☐ COPY OF PRE-APPLICATION COMMENTS. IF YOU HAVE NOT HAD A PRE-APPLICATION MEETING TO DISCUSS THIS PROJECT PLEASE CONTACT THE CITY PLANNER TO ARRANGE AN APPOINTMENT AT 386-248-9424.
- ☑ ELECTRONIC COPY OF ALL ITEMS SUBMITTED
- ☑ APPLICATION AND FEE
- ☑ PROOF THAT TAXES ARE CURRENT
- ☑ PROPERTY APPRAISER'S PROPERTY INFORMATION PRINTOUT
- ☑ OWNERSHIP DISCLOSURE FORM (ADD'L DOCUMENTATION MAY REQUIRED IF OWNER IS A TRUST OR CORPORATION)
- ☑ OWNER'S AUTHORIZATION FORM, IF APPLICABLE (ADD'L DOCUMENTATION REQUIRED IF OWNER IS A TRUST OR CORPORATION)
- ☑ 2 CURRENT SIGNED AND SEALED BOUNDARY SURVEYS
- ☑ LEGAL DESCRIPTION IN MS WORD FORMAT (EMAIL THIS TO THE CITY PLANNER)
- ☒ SCHOOL CAPACITY REVIEW – *IF PROPOSING OVER 10 RESIDENTIAL UNITS (CONTACT SCHOOL BOARD PLANNING & BUSINESS SERVICES AT 386-734-7190 FOR APPLICATION)*

Attachment: PUD application with parcel information sheets (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

HOLLY HILL
FLORIDA
1065 Ridgewood Avenue, Holly Hill, FL 32117
Phone: (386) 248-9442 Fax: (386) 248-9498 Permitdesk@hollyhillfl.org 01/2023

- [x] TRAFFIC IMPACT ANALYSIS FOR PROJECTS GENERATING OVER 1000 TRIPS PER DAY ACCORDING TO RATES PUBLISHED BY THE INSTITUTE OF TRANSPORTATION ENGINEERS "TRIP GENERATION MANUAL" (LATEST EDITION)
- [x] DRAFT DEVELOPMENT ORDER IN MS WORD FORMAT (*PD REZONE ONLY – CONTACT THE CITY PLANNER)*
- [x] PRELIMINARY DEVELOPMENT PLAN (***PD REZONE ONLY*** - *SEE CODE SEC. 114-771*)
- [x] **REZONES ONLY**: ANSWER THE 8 QUESTIONS ATTACHED ON THE REZONING REQUIREMENTS SHEET
- [ ] **COMPREHENSIVE PLAN AMENDMENTS ONLY**: Provide a **Facility Demand Comparison**. For example, for the existing Future Land Use designation, show the demands on the city's infrastructure at the highest intensity, and for the proposed Future Land Use, show what the demands would be at the highest intensity. Show this information for the following facilities:
  - Potable Water
  - Sanitary Sewer
  - Stormwater
  - Transportation (Use current year ITE Trip Generation Rates–Provide PM Peak Hour and Avg Daily)
  - Solid Waste Collection
  - School (Residential Only)
- [ ] **COMPREHENSIVE PLAN AMENDMENTS ONLY**: Provide a **Demonstration of Capacity**: Show that there is capacity and ability to meet increased demands on facilities. The city's public works department can assist in providing information regarding potable water, sanitary sewer and solid waste.

Applicant's Signature: _____ 04/22/24
(Signature) *(Date)*

Nika Hosseini
(Print)

Applications must be complete to initiate the review process. For questions please contact the City Planner at (386) 248-9424, fax (386) 248-9498 or email at bwalker@hollyhillfl.org

Attachment: PUD application with parcel information sheets (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

KBL Property Investments, LLC

Parcel Information List

Parcel ID No.:	5337-23-00-0041
Parcel Address:	Mason Ave., Holly Hill, FL 32117
Property Owner:	KBL Property Investments, LLC PO Box 148 Flagler Beach, FL 32136

Parcel ID No.:	5337-23-00-0050
Parcel Address:	148 Mason Ave., Holly Hill, FL 32117
Property Owner:	KBL Property Investments, LLC PO Box 148 Flagler Beach, FL 32136

Parcel ID No.:	5337-23-00-0061
Parcel Address:	Daytona Ave., Holly Hill, FL 32117
Property Owner:	KBL Property Investments, LLC PO Box 148 Flagler Beach, FL 32136

Parcel ID No.:	5337-23-00-0070
Parcel Address:	105 Daytona Ave., Holly Hill, FL 32117
Property Owner:	KBL Property Investments, LLC PO Box 148 Flagler Beach, FL 32136

Parcel ID No.:	5337-23-00-0080
Parcel Address:	148 Mason Ave., Holly Hill, FL 32117
Property Owner:	KBL Property Investments, LLC PO Box 148 Flagler Beach, FL 32136

Parcel ID No.:	5337-22-01-0010
Parcel Address:	155 1st St., Holly Hill, FL 32117
Property Owner:	KBL Property Investments, LLC PO Box 148 Flagler Beach, FL 32136

Parcel ID No.:	5337-22-01-0011
Parcel Address:	151 1st St., Holly Hill, FL 32117

Attachment: PUD application with parcel information sheets (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

Property Owner: KBL Property Investments, LLC
PO Box 148
Flagler Beach, FL 32136

Parcel ID No.: 5337-22-01-0020
Parcel Address: 149 1st St., Holly Hill, FL 32117
Property Owner: KBL Property Investments, LLC
PO Box 148
Flagler Beach, FL 32136

Attachment: PUD application with parcel information sheets (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

Charlesdale Associates, Inc.

Parcel Information List

Parcel ID No.:	5337-22-01-0021
Parcel Address:	145 1st Street, Holly Hill, FL 32117
Property Owner:	Charlesdale Associates, Inc. 134 Mason Ave. Daytona Beach, FL 32117

Parcel ID No.:	5337-23-00-0020
Parcel Address:	140 Mason Ave., Holly Hill, FL 32117
Property Owner:	Charlesdale Associates, Inc. 134 Mason Ave. Daytona Beach, FL 32117

Parcel ID No.:	5337-25-00-0060
Parcel Address:	134 Mason Ave., Holly Hill, FL 32117
Property Owner:	Charlesdale Associates, Inc. 134 Mason Ave. Daytona Beach, FL 32117

Parcel ID No.:	5337-25-00-0011
Parcel Address:	120 Mason Ave., Holly Hill, FL 32117
Property Owner:	Charlesdale Associates, Inc. 134 Mason Ave. Daytona Beach, FL 32117

Attachment: PUD application with parcel information sheets (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

HOLLY HILL
FLORIDA
1065 Ridgewood Avenue, Holly Hill, FL 32117
Phone: (386) 248-9442 Fax: (386) 248-9498 Permitdesk@hollyhillfl.org

01/2023

REZONING REQUIREMENTS

The following items must be completed in sufficient detail to allow the City to determine if the application complies with the City Code Chapter 114 and Section 82-372.

1. Is it consistent with all adopted elements of the comprehensive plan? [X]YES []NO Explain.

The intended use of the site clearly matches the land use in the surrounding area.

2. What is its impact upon the environment or natural resources? []YES []NO Explain.

The subject property is not heavily wooded and does not have any wetlands on site. The subject site is in between a gas station and an automobile service station.

3. What is its impact upon the economy of any affected area? []YES []NO Explain.

The property is currently vacant, undeveloped land that has not been utilized. By developing the property, it will increase the value of the subject land and the surrounding area.

4. What is its impact upon any existing necessary governmental services such as schools, sewage disposal, solid waste or transportation systems? []YES []NO Explain.

It is a commercial development and as such, does not have an impact on schools. Regarding transportation, the intended use of the site is a storage facility which is the lowest generator of vehicular traffic. The solid waste and sewage systems will be minimally impacted due to the nature of the use as a self storage facility.

5. Are there any changes in circumstances or conditions affecting the area.? []YES [X]NO

Attachment: Rezoning Requirements (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

HOLLY HILL
FLORIDA
1065 Ridgewood Avenue, Holly Hill, FL 32117
Phone: (386) 248-9442 Fax: (386) 248-9498 Permitdesk@hollyhillfl.org 01/2023

Explain.

No. We are looking to develop the property.

6. Are there any mistakes in the original classification? ☐YES ☒NO Explain.

No. this is a PD Agreement in order to accommodate a storage facility.

7. What is its effect upon the use or value of the affected area? ☐YES ☐NO Explain.

The property is currently vacant, undeveloped land that has not been utilized. By developing the property, it will increase the value of the subject land and the surrounding area.

8. What is its impact upon the public health, welfare, safety or morals? ☐YES ☐NO Explain.

The subject property is not heavily wooded and does not have any wetlands on site. The subject site is in between a gas station and an automobile service station. A storage facility fits well in the general area of the neighborhood.

Nika Hosseini
Print Applicant Name

Applicant Signature

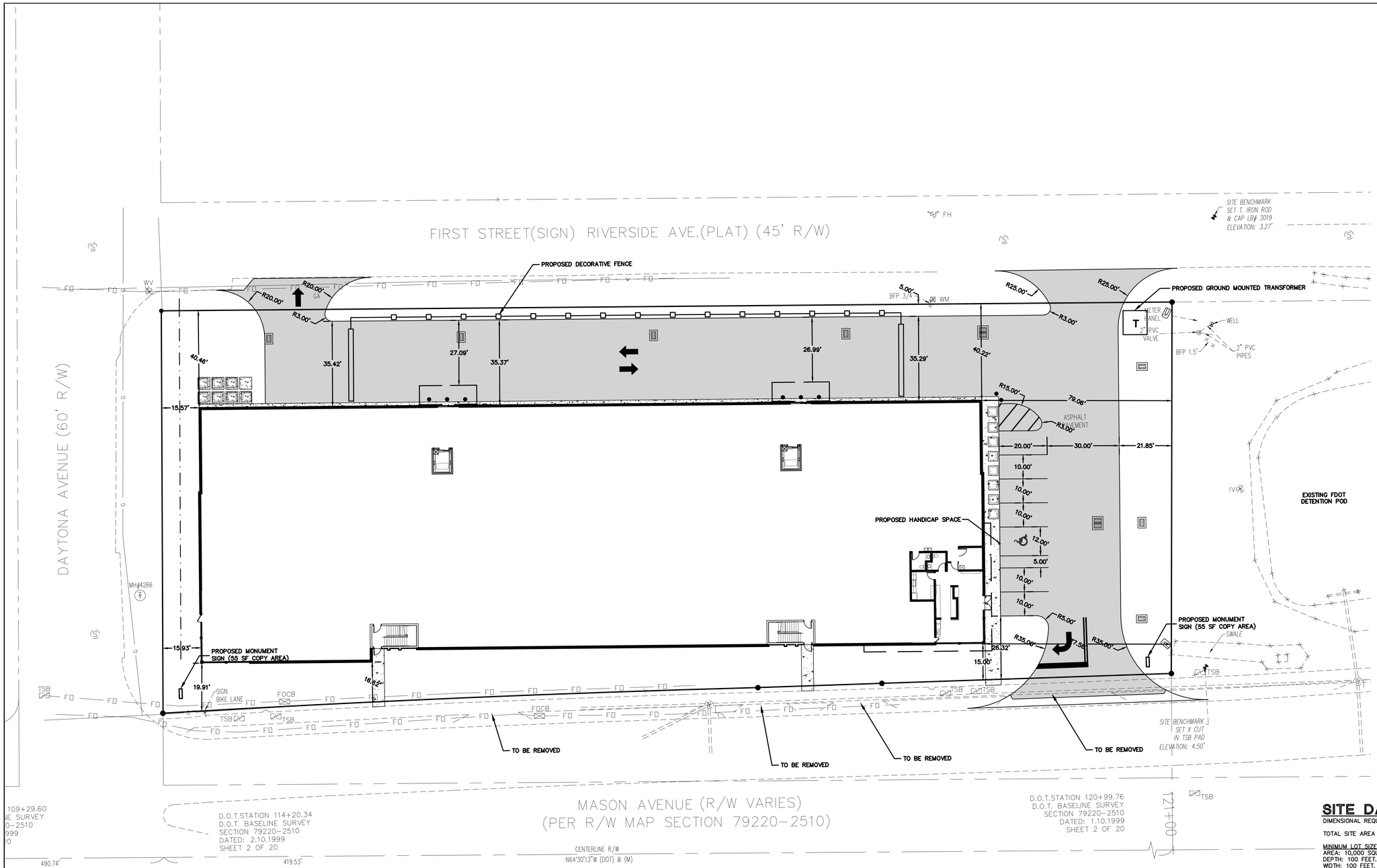
Print Applicant Name

Applicant Signature

04/22/24
Date

Date

Attachment: Rezoning Requirements (2024-O-3079 : Mason Avenue Storage Facility Planned Development)



NO.	DATE	DESCRIPTION	BY
		REVISIONS	
1	4/18/2024	REVISED	MAG
2	6/25/2024	REVISED	MAG
3	6/26/2024	REVISED SIGN AREA	MAG
4	6/27/2024	REVISED	MAG
5	8/22/2024	REVISED SITE DATA TABLE	MAG

PARKER MYNCHENBERG & ASSOCIATES, INC.
PROFESSIONAL ENGINEERS * LANDSCAPE ARCHITECTS
1729 RIDGEWOOD AVENUE HOLLY HILL, FLORIDA 32117
(386) 677-6891 FAX (386) 677-2114 E-MAIL: info@parkermynchenberg.com
PARKER MYNCHENBERG P.E. #32645 R.L.A. #0001553, STEVE BUSWELL P.E. #53985 R.L.A. #A6667011
CERTIFICATE OF AUTHORIZATION NUMBER 00003910

148 MASON AVENUE
HOLLY HILL * FLORIDA

CONCEPTUAL SITE PLAN

1
SHEET NO.

Drawn By: M .GRECO
Date: 02/20/2024
JOB #
SCALE: 1"=20'

SEAL

SITE DATA TABLE:

DIMENSIONAL REQUIREMENTS IN THE PD ARE AS FOLLOWS:

TOTAL SITE AREA = 67,246 SF = 1.544 ACRES

MINIMUM LOT SIZE:
AREA: 10,000 SQUARE FEET.
DEPTH: 100 FEET.
WIDTH: 100 FEET.

MINIMUM BUILDING SETBACKS:
SOUTH (MASON AVE) = 15 FT
WEST (DAYTONA AVE) = 15 FT
EAST (PARKING AREA) = 10 FT
NORTH (1ST STREET) = 40 FT

MINIMUM LANDSCAPE BUFFERS:
SOUTH (MASON AVE) = 15 FT
WEST (DAYTONA AVE) = 15 FT
EAST (PARKING AREA) = 10 FT
NORTH (1ST STREET) = 5 FT

PROPOSED BUILDING HEIGHT = 40 FEET.

PROPOSED BUILDING LOT COVERAGE = 33,262/67,246 = 49.46%

PROPOSED OPEN SPACE = 21.29%

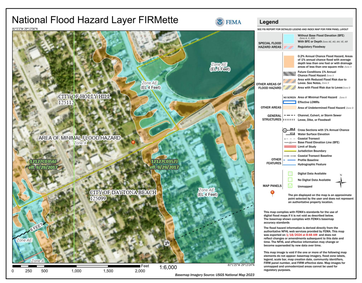
FLOOR AREA RATIO (FAR)
PROPOSED FAR = 33,262 * 3/67,246 = 1.48

*THE PROPERTY IS LOCATED WITHIN THE UTILITY SERVICE AREA FOR THE CITY OF HOLLY HILL

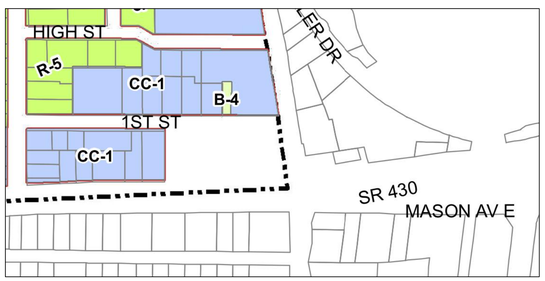
PARKING CALCULATIONS:

PARKING PROVIDED:

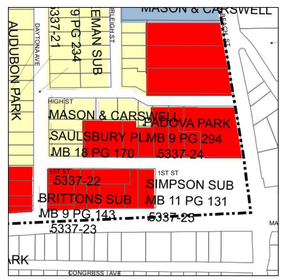
STANDARD.....6 SPACES
HANDICAPPED.....1 SPACES
TOTAL.....7 SPACES



FEMA FLOOD ZONE MAP



EXISTING ZONING MAP



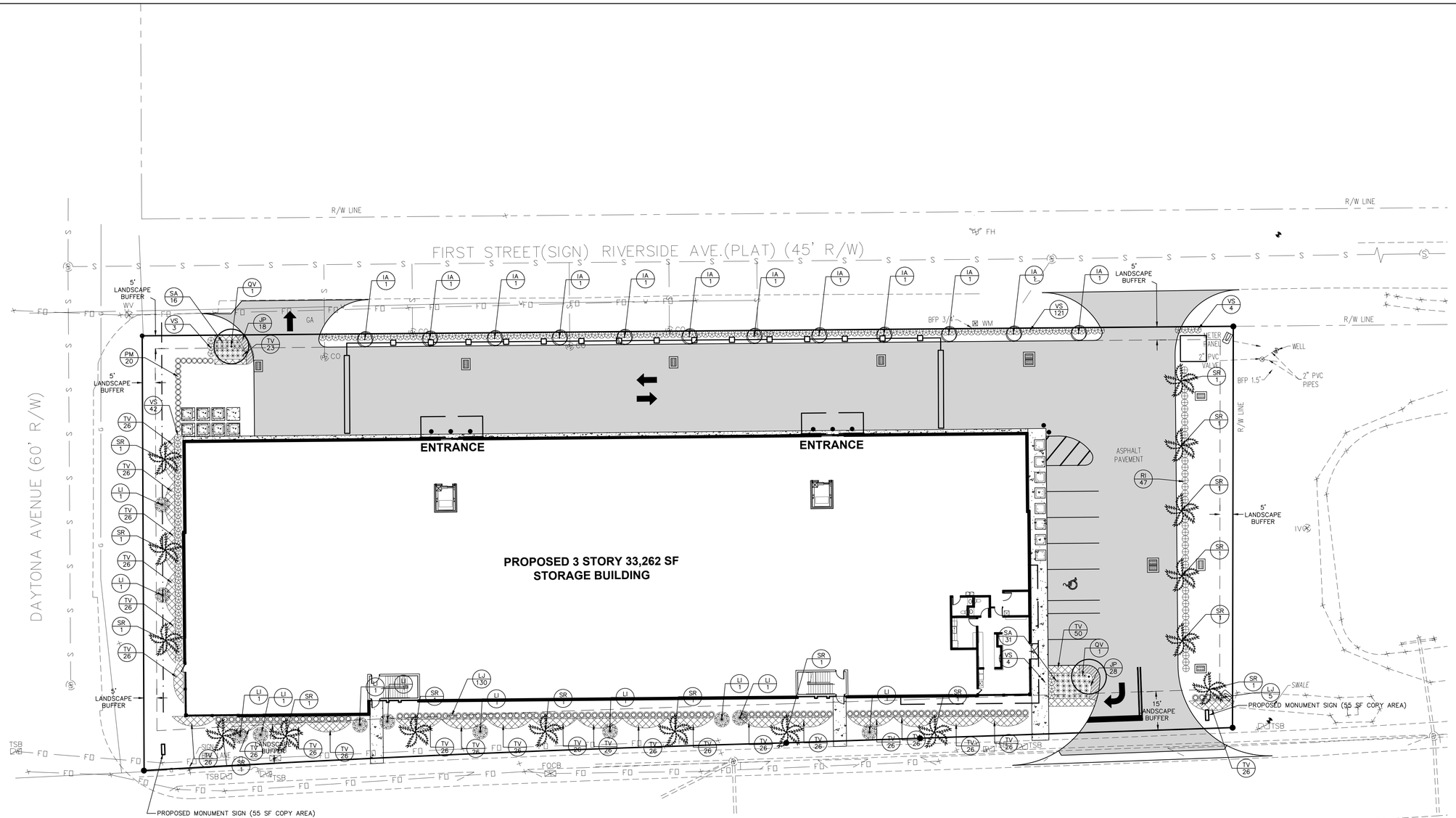
FUTURE LAND USE MAP



AERIAL MAP

Attachment: Concept Plan (rev 8-23-2024) (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

GRAPHIC SCALE
0 10 20 40 60
SCALE: 1" = 20'



PLANT LIST

SYMBOL	ABB.	QTY.	BOTANICAL NAME	COMMON NAME	SIZE
	QV	2	QUERCUS VIRGINIANA	LIVE OAK	10'-12' HT. 2.5" MIN. CAL.
	SR	16	SYAGRUS ROMANZOFFIANA	QUEEN PALM	10'-12' HT.
	LI	10	LAGERSTROEMIA INDICA	CREPE MYRTLE	45 GAL., 8' HT. STANDARD TRUNK 2.5" MIN. CAL.
	JP	64	JUNIPEROUS "PARSONII"	PARSON'S JUNIPER	1 GAL., 12"-15" SPD. 18" O.C.
	TV	749	TULBAGHIA VIOLACEA	SOCIETY GARLIC	1 GAL., 12"-15" SPD., 20" O.C.
	RI	47	RAPHIOLEPIS INDICA	INDIAN HAWTHORN (WHITE VARIETY)	3 GAL., 30" O.C. 24" HT., MIN.
	VS	174	VIBURNUM SUSPENSUM	SANDANKA VIBURNUM	3 GAL., 30" O.C. 24" HT., MIN.
	PM	20	PODOCARPUS MACROPHYLLUS	YEW PODOCARPUS	3 GAL., 30" O.C. 24" HT., MIN.
	LJ	136	LIGUSTRUM JAPONICUM	LIGUSTRUM	3 GAL., 30" O.C. 24" HT., MIN.
	SA	53	SCHEFFLERA ARBORICOLA "TRINETTE"	VARIEGATED ARBORICOLA	3 GAL., 30" O.C. 24" HT., MIN.
	IA	12	ILEX X ATTENUATA "EAGLESTON"	EAGLESTON HOLLY	30 GAL., MIN. 8' HT 1.5" CAL.
SOD	ARGENTINE BAHIA SOD (SQ. FT.), UNLESS NOTED OTHERWISE ON PLANS				

NO.	DATE	DESCRIPTION	BY
		REVISIONS	
5	8/22/2024	REVISED SITE DATA TABLE	MAG
4	6/27/2024	REVISED	MAG
3	6/26/2024	REVISED SIGN AREA	MAG
2	6/25/2024	REVISED	MAG
1	4/18/2024	REVISED	MAG

PARKER MYNCHENBERG & ASSOCIATES, INC.
PROFESSIONAL ENGINEERS * LANDSCAPE ARCHITECTS
1729 RIDGEWOOD AVENUE HOLLY HILL, FLORIDA 32117
(386) 677-6891 FAX (386) 677-2114 E-MAIL: info@parkermynchenberg.com
PARKER MYNCHENBERG P.E. #32645 R.L.A. #0001553, STEVE BUSHELL P.E. #53985 R.L.A. #A6667011
CERTIFICATE OF AUTHORIZATION NUMBER 00003910

148 MASON AVENUE
HOLLY HILL * FLORIDA

CONCEPTUAL LANDSCAPE PLAN

1
SHEET NO.

Drawn By: M .GRECO
Date: 02/20/2024
JOB #
SCALE: 1"=20'

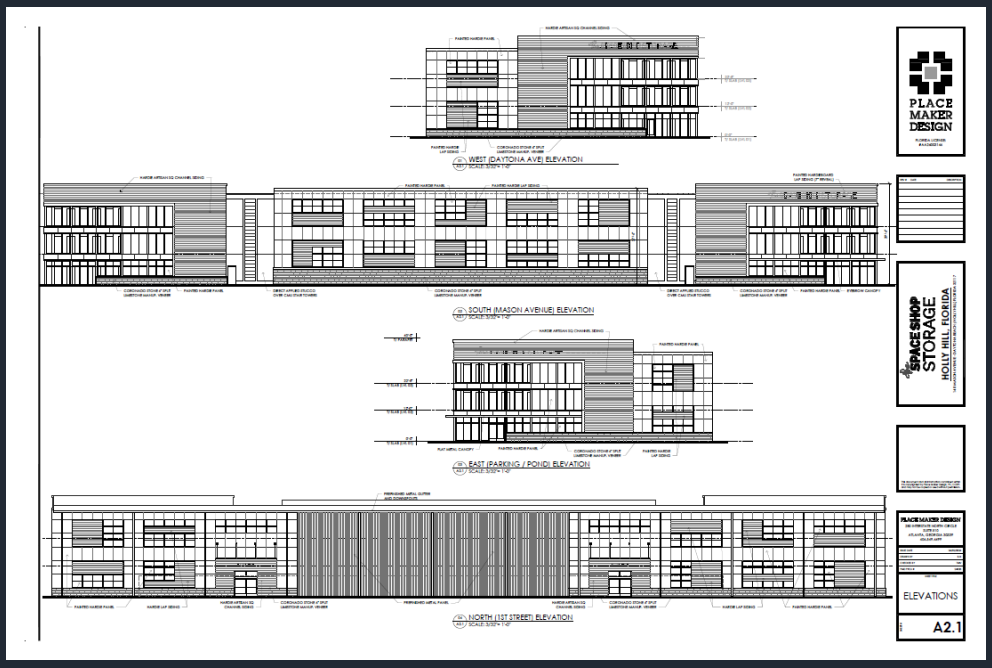
SEAL

Attachment: Landscape Plan (rev 8-23-2024) (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

Renderings and Elevation







Attachment: Renderings and Elevation (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

Table 1: Land Use and Zoning Table

Mason Avenue Storage

	Existing Development	Future Land Use Designation	Zoning Classification
Site	**Vacant Land and Building**	**Commercial**	**CC-1**
North	**Single Family Homes & Vacant Land**	**Commercial and Low Density Residential**	**CC-1 and R-5**
South	**Mason Ave and Single Family Homes (Volusia County)**	**Volusia County**	**Volusia County**
East	**Pond**	**Pond**	**Pond**
West	**Business and Single-Family Home**	**Commercial**	**CC-1**

Attachment: Land Use and Zoning Table (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

11-2022

Exhibit to Ordinance No. _____

DEVELOPMENT AGREEMENT for the project known as 148 Mason Avenue Planned Unit Development (PUD) located at the corner of Mason Avenue and Daytona Avenue in Holly Hill, Florida (hereinafter referred to as the "Subject Property").

THIS DEVELOPMENT AGREEMENT (hereinafter referred to as the "Agreement") is entered into and made as of the ___ day of _____, 20____, by and between the **CITY OF HOLLY HILL**, a Florida municipal corporation, with a mailing address of 1065 Ridgewood Ave. Holly Hill, FL 32117 (hereinafter referred to as the "City"), **KBL PROPERTY INVESTMENTS, LLC**, a Florida limited liability company, whose mailing address is P.O. Box 148, Flagler Beach, FL 32136, **CHARLESDALE ASSOCIATES, INC.,** a Florida profit corporation, whose mailing address is P.O. Box 148, Flagler Beach, FL 32136 (hereinafter referred to as the "Owners"), and **STEIN INVESTMENT CO, LLC**, a Foreign limited liability company, whose mailing address is 5607 Glenridge Dr., NE, Suite 200, Atlanta, GA 30342 (hereinafter referred to as the "Developer").

W I T N E S S E T H

WHEREAS, the Owners warrant that they holds legal title to the lands located in Volusia County, Florida, and within the corporate limits of the City of Holly Hill, said lands being more particularly described in **Exhibit "A"**, Legal Description for the Subject Property, attached hereto and by this reference made a part hereof; and that the holders of any and all liens and encumbrances affecting such property will subordinate their interests to this Agreement; and

WHEREAS, the Owners/Developer have clear title of the Subject Property and the Developer is currently under contract to purchase the Subject Property and intends to develop such property; and

WHEREAS the Owners/Developer desire to facilitate the orderly development of the Subject Property in compliance with the laws and regulations of the City and of other governmental authorities, and the Owners/Developer desire to ensure that its development is compatible with other properties in the area and planned traffic patterns; and

WHEREAS the development permitted or proposed under this Development Agreement is consistent with the City's Comprehensive Plan, concurrency management system, and all land development regulations; and

WHEREAS it is the purpose of this Agreement to clearly set forth the understanding and agreement of the parties concerning the matters contained herein; and

WHEREAS the Owners/Developer has sought the City's approval to develop the Subject

Attachment: Development Agreement (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

Property, and the City approved **Ordinance No.** _____, through rezoning the Subject Property to a form of Planned Unit Development (PUD), as defined under the City's Land Development Code; and

WHEREAS, the PUD shall consist of this Agreement as the Written Development Agreement of the PUD, and a Preliminary Plan also known as the Preliminary Development Plan, attached hereto as **Exhibit, "B"**, subject to the covenants, restrictions, and easements offered by the Owner/Developer and contained herein, (hereinafter the "Master Development Plan"). Where more detailed criteria for City required submittals exceed the criteria required for a Master Development Plan, the more detailed criteria apply.

NOW THEREFORE, in consideration of the mutual covenants and agreements contained herein, and other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the parties hereto agree as follows:

1. **Recitals and Definitions.** The recitals herein contained are true and correct and are incorporated herein by reference. All capitalized terms not otherwise defined herein shall be as defined or described in the City's Land Development Code as it may be amended from time to time, unless otherwise indicated.

2. **Title Opinion/Certification.** The Developer will provide to the City, in advance of the City's execution and recordation of this Agreement, a title opinion from a licensed attorney in the state of Florida, or a certification by an abstractor or title company authorized to do business in the state of Florida, verifying marketable title to the Subject Property to be in the name of the Owner/Developer and any and all liens, mortgages, and other encumbrances that are either satisfied or not satisfied or released of record. A unity of title agreement may be executed to ensure the property is held by the Owners pending development as proposed by this Agreement.

3. **Subordination/Joinder.** Unless otherwise agreed to by the City and if applicable, all liens, mortgages, and other encumbrances that are not satisfied or released of record, must be subordinated to the terms of this Agreement or the Lienholder join in this Agreement. It shall be the responsibility of the Owner/Developer to promptly obtain the said subordination or joinder, in a form and substance that is acceptable to the City Attorney, prior to the execution and recordation of this Agreement.

4. **Duration.** The duration of this Agreement is binding and runs with the land in perpetuity, unless amended.

5. **Development of the Subject Property**. Development of the Subject Property shall be subject to performance standards listed in this Agreement. Where a land use listed below differs from a defined use in the City of Holly Hill's Code of Ordinances, the use listed in this Agreement

Attachment: Development Agreement (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

shall prevail.

A. Permitted principal uses allowable on the Subject Property:
- Administrative offices.
- Business services.
- General office uses.
- Mini warehouses.
- Self-service storage facilities.
- Personal services.
- Professional services offices.
- Uses customarily associated with, dependent on and incidental to the permitted principal use.

B. Prohibited principal uses, if any:
1. Unless a use is specifically stated as permitted, it is prohibited.

C. Subject Property Size: Approximately 1.544 +/- acres.

D. Maximum FAR: 1.5.

E. Impervious surface is not to exceed 80% of the gross square footage for the Subject Property, as illustrated on Exhibit "B".

F. Minimum landscape buffer-yard requirements:
1. South Buffer Width (Mason Ave) - 15 feet
2. West Buffer Width (Daytona Ave) - 15 feet
3. East Buffer Width (Parking Area) - 10 feet
4. North Buffer Width (1st Street) - 5 feet

G. Maximum building length: 325 ft.

H. Minimum lot width (in feet): 100 ft.

I. Maximum lot coverage: 50%.

J. Minimum building setbacks:
1. South Setback (Mason Ave) - 15 feet
2. West Setback (Daytona Ave) - 15 feet
3. East Setback (Parking Area) - 10 feet
4. North Setback (1st Street) - 40 feet

Attachment: Development Agreement (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

K. Maximum building height (in feet): 40 feet.

L. Minimum parking standards are as shown and stated on the Preliminary Plan.

M. The project shall consist of 1 phase.

N. Architectural controls and development on the Subject Property shall follow a common architectural theme as listed in this Agreement by harmoniously coordinating the general appearance of all buildings and accessory structures.

O. Utility provision and dedication: The Owners/Developer shall connect to the City of Holly Hill's central utility systems when available, or to another approved utility provider where applicable, at their sole cost and expense. Utility fees shall be paid to City of Holly Hill or to the applicable utility provider.

P. Stormwater and environmental: Per parcel stormwater systems or master stormwater systems shall be owned and maintained by an established Property Owner's Association, or by the property owner in private ownership, and shall not be dedicated to or become the responsibility of the City of Holly Hill. All environmental permitting, mitigation, and/or soil and erosion control for the property shall conform to all federal, state, and local permits/requirements, and shall be the sole responsibility of the Property Owner's Association, or by the property owner, and shall be maintained in good condition/standing with the applicable permitting authorities. Best Management Practices and conformance to National Pollutant Discharge Elimination System (NPDES) criteria are required.

Q. Transportation, site access, and traffic devices: The Owners/Developer are responsible for all transportation improvements within the Subject Property and any off-site transportation improvements required because of the proposed development, for site function, which maintains or improves the level of service for area roadways, and ensures the public health, safety, and welfare for the community. All permits shall be obtained from appropriate permitting agencies prior to development and the City shall determine the appropriate level of service per the City Comprehensive Plan and current traffic counts.

R. The development criteria set forth in this Section 5 shall apply to configuration of the Property in its current configuration. In the event that additional right-of-way is needed for dedication to Volusia County, such dedication shall not impact the development footprint for the Property, which shall be measured from the existing site boundaries.

S. Minor adjustments to the development criteria for lot width, buffer width, and minimum setbacks set forth in this Section 5 shall be permitted as minor amendments,

Attachment: Development Agreement (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

so long as such adjustments do not exceed 10% of any of the stated criteria, and shall not impact the general intent and character of the approved project.

T. The project shall provide a minimum of 19% of open space.

6. **Development Permits/Fees.** The Owners/Developer are responsible for obtaining permitting, and the payment of all fees for facilities and services for the Subject Property. Any site permits shall be kept current with the respective permitting agency and shall ensure the protection of the public health, safety, and welfare of the community and the development. All impact fees are applicable, and no impact fee credits shall be awarded through this Agreement; unless a cessation exists through a City moratorium that is Citywide. Proportionate fair share site improvements shall not be used in lieu of impact fees.

7. **Site Plan/Plat Approval.** The Master Development Plan, is the Preliminary Plan and this Written Development Agreement. The Master Development Plan shall not replace, supersede, or absolve the Owners/Developer from approvals for any site plan, preliminary plat, and/or final plat and their respective regulations. Where more detailed criteria for City required submittals exceed the criteria required for a Master Development Plan, the more detailed criteria apply.

8. **Indemnification.** The Owners/Developer shall indemnify and hold the City harmless from any and against all claims, demands, disputes, damages, costs, expenses, (to include attorneys' fees whether or not litigation is necessary and if necessary, both at trial and on appeal), incurred by the City as a result, directly or indirectly, of the use or development of the Subject Property, except those claims or liabilities caused by or arising from the negligence or intentional acts of the City, or its employees or agents. It is specifically understood that the City is not guaranteeing the appropriateness, efficiency, quality or legality of the use or development of the Subject Property, including but not limited to, drainage or water/sewer plans, fire safety, or quality of construction, whether inspected, approved, or permitted by the City.

9. **Compliance.** The Owners/Developer agree that it, and their successors and assigns, will abide by the provisions of this Agreement, the City's Comprehensive Plan and the City's Code of Ordinances, including but not limited to, the site plan regulations of the City as amended from time to time, which are incorporated herein by reference and such subsequent amendments hereto as may be applicable. Further, all required improvements, including landscaping, shall be continuously maintained by the Owners/Developer, or their successors and assigns, in accordance with the City's Code of Ordinances. The City may, without prejudice to any other legal or equitable right or remedy it may have, withhold permits, Certificates of Occupancy, or plan/plat approvals to the Subject Property, should the Owners/Developer fail to comply with the terms of this Agreement. In the event of a conflict between this Development Agreement and the City's Land Development Code, the more restrictive regulations shall govern the development of the Subject Property.

Attachment: Development Agreement (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

10. **Obligations for Improvements.** Any surface improvement as described and required hereunder included, but not limited to such as signalization, walls, stormwater management facilities, medians, and utilities, or any other surface improvement shall be performed prior to the issuance of the first Certificate of Occupancy on that portion of the Subject Property that the surface improvement(s) relates or is otherwise scheduled in this Agreement. Should the Owners/Developer fail to undertake and complete its obligations as described in this Agreement and to the City's specifications, then the City shall give the Owners/Developer thirty (30) days written notice to commence and ninety (90) days to complete said required obligation at the sole expense of the Owners/Developer. If the Owners/Developer fails to complete the obligations within the ninety (90) day period, then the City, without further notice to the Owners/Developer and their successors and assigns in interest, may but shall not be required to, perform such obligations at the expense of the Owners/Developer or their successors and assigns in interest, without prejudice to any other rights or remedies the City may have under this Agreement. Further, the City is hereby authorized to immediately recover the actual and verified cost of completing the obligations required under this Agreement and any legal fees from the Owners/Developer in an action at law for damages, as well as record a lien against the Subject Property in that amount. The lien of such assessments shall be superior to all others, and all existing lienholders and mortgagees. Notice to the Owners/Developer and their successors and assigns in interest shall be deemed to have been given upon the mailing of notice as provided in **paragraph (16)** of this Agreement.

11. **Environmental and Tree Preservation.** The Owners/Developer is responsible to obtain all site related permits and approval prior to any development activity on or for the Subject Property. This may involve mitigation for habitat of threatened or endangered flora and fauna or species identified for protection (i.e., tree preservation). This Agreement does not vest or exempt the Owners/Developer from any permitting and mitigation obligations needed to develop a Subject Property.

12. **Homeowners Association or Property Owners Association.** The charter and by-laws of any Property Owner's Association ("POA") for the Subject Property and any deed restrictions related thereto shall be furnished to the City for approval by the City Attorney prior to the recording thereof in the Public Records of Volusia County, Florida. Such recording shall take place before a Certificate of Occupancy is issued for the first development project on land covered by this Agreement. The POA shall at a minimum be responsible for maintaining the common open space, any common utility systems, such as for irrigation and site lighting, and project signage. The Owners/Developer shall be responsible for establishing the POA and recording said information in the Public Records of Volusia County, Florida. The City is not responsible for the enforcement of any agreements or deed restrictions entered into between property owners or occupiers of the Subject Property. If maintenance for the Subject Property is not maintained following issuance of a Certificate of Occupancy, the property owner shall be subject to code enforcement.

Attachment: Development Agreement (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

13. **Enforcement.** Both parties may seek specific performance of this Agreement and/or bring an action for damages in a court within Volusia County, Florida, if either party breaches this Agreement. If enforcement of this Agreement by the City becomes necessary, and the City is successful in such enforcement, the Owners/Developer shall be responsible for the payment of all the City's costs and expenses, including attorney fees, whether or not litigation is necessary and, if necessary, both at trial and on appeal. Such costs, expenses and fees shall also be a lien upon the Subject Property superior to all others. Should this Agreement require the payment of any monies to the City, the recording of this Agreement shall constitute a lien upon the Subject Property for said monies, until said are paid, in addition to such other obligations as this Agreement may impose upon the Subject Property and the Owners/Developer. Interest on unpaid overdue sums shall accrue at the rate of the lesser of eighteen percent (18%) compounded annually or at the maximum rate allowed by law.

14. **Utility Easements.** For any easement not established on a plat for the Subject Property, the Owners/Developer shall provide to the City such easements and other legal documentation, in a form mutually acceptable to the City Attorney and the Owners/Developer, as the City and Developer may deem reasonably necessary or appropriate for the installation and maintenance of the utility and other services, including but not limited to, sanitary sewer, potable water, and reclaimed water services, electric, cable, gas, fire protection and telecommunications.

15. **Periodic Review.** The City reserves the right to review the Subject Property in relation to this Agreement periodically to determine if there has been demonstrated good faith compliance with the terms of this Agreement. If the City finds that based on substantial competent evidence that there has been a failure to comply with the terms of this Agreement, the City may not issue development orders or permits until compliance with this Agreement has been established.

16. **Notices.** Where notice is herein required to be given, it shall be by certified mail return receipt requested, hand delivery or nationally recognized courier, such as Federal Express or UPS. E-mail delivery of documents shall not replace or be in lieu of the aforementioned process. Said notice shall be sent to the following, as applicable:

OWNERS/DEVELOPER'S REPRESENTATIVES:

KBL Property Investments, LLC (Owner)
Attn: Robert Goldberg
P.O. Box 148
Flagler Beach, FL 32136

With Copy To: Cobb Cole Law Firm
Attn: Mark A. Watts, Esq.
231 N. Woodland Blvd.
DeLand, FL 32720

Attachment: Development Agreement (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

Charlesdale Associates, Inc. (Owner)
Attn: Robert Goldberg
P.O. Box 148
Flagler Beach, FL 32136

Stein Investment Co, LLC (Developer)
Attn: Daniel Ginburg
5607 Glenridge Dr., NE, Suite 200
Atlanta, GA 30342

CITY'S REPRESENTATIVES:
City Manager
City of Holly Hill
1065 Ridgewood Ave.
Holly Hill, Florida 32117

With copy to:

Director
Community Development
City of Holly Hill
1065 Ridgewood Ave.
Holly Hill, Florida 32725

Should any party identified above change, it shall be said party's obligation to notify the remaining parties of the change in a fashion as is required for notices herein. It shall be the Owners/Developer's obligation to identify its lender(s) to all parties in a fashion as is required for notices herein.

17. **Compliance with the Law.** The failure of this Agreement to address a particular permit, condition, term, or restriction shall not relieve the Owners/Developer of the Subject Property from the necessity of complying with the law governing said permitting requirements, conditions, terms, or restrictions.

18. **Captions.** The captions used herein are for convenience only and shall not be relied upon in construing this Agreement.

19. **Binding Effect.** This Agreement shall run with the land, and shall be binding upon and inure to the benefit of the Owner/Developer and their successors and assigns in interest, and the City and their successor and assigns in interest. This Agreement shall become effective upon its execution and recordation with the Public Records of Volusia County, Florida. This Agreement does not, and is not intended to, prevent, or impede the City from exercising its legislative authority as the same may affect the Subject Property.

20. **Subsequently Enacted State or Federal Law.** If either state of federal law is enacted after the effective date of this Agreement that is applicable to and precludes the parties' compliance with the terms of this Agreement, this Agreement and correlating zoning amendment

Attachment: Development Agreement (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

shall be modified or revoked, as is necessary, to comply with the relevant state or federal law.

21. **Severability.** If any part of this Development Agreement is found invalid or unenforceable in any court, such invalidity or unenforceability shall not affect the other parts of this Development Agreement if the rights and obligations of the parties contained herein are not materially prejudiced and if the intentions of the parties can be effected. To that end, this Development Agreement is declared severable.

22. **Covenant Running with the Land.** This Agreement shall run with the Subject Property and inure to and be for the benefit of the parties hereto and their respective successors and assigns and any person, firm, corporation, or entity who may become the successor in interest to the Subject Property or any portion thereof.

23. **Recordation of Agreement.** The parties hereto agree that an executed original of this Agreement shall be recorded by the City, at the Developer's expense, in the Public Records of Volusia County, Florida.

24. **Applicable Law/Venue.** This Agreement and the provisions contained herein shall be construed, controlled, and interpreted according to the laws of the State of Florida. Venue of any litigation relating to this Agreement shall be in the courts of Volusia County, Florida.

25. **Time of the Essence.** Time is hereby declared of the essence to the lawful performance of the duties and obligations contained in this Agreement. The Owners/Developer shall execute this Agreement within ten (10) business days of City Commission adoption and agrees to pay the cost of recording this document in the Public Records of Volusia County, Florida. Failure to execute this Agreement within ten (10) business days of this ordinance adoption may result in the City not issuing development orders or permits until execution and recordation of this Agreement has occurred.

26. **Agreement; Amendment.** This Agreement constitutes the entire agreement between the parties, and supersedes all previous discussions, understandings, and agreements, with respect to the subject matter hereof; provided however, that it is agreed that this Agreement is supplemental to the City's Comprehensive Plan and does not in any way rescind or modify any provisions of the City's Comprehensive Plan. Amendments to and waivers of the provisions of this Agreement shall be made by the parties only in writing by formal amendment.

27. **Amendments.** Amendments to the Master Development Plan (MDP) shall be subject to the requirements of Section 114-771(g)(4) of the City of Holly Hill Land Development Regulations, which state that minor amendments to the Preliminary Plan not violating any terms of the written development agreement and not altering the intent and purpose of the MDP may be approved by the Development Code Administrator after such departmental comment as he/she deems appropriate. Minor changes shall be limited to items such as small adjustments to building

Attachment: Development Agreement (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

footprints, allocation of uses within a defined parcel such as retention areas, parking etc. Major amendments will require full review and shall include relocation of uses on the site, except as permitted by the MDP, changes to building styles, changes to landscaping requirements, etc. Decisions as to whether modifications are Major or Minor shall be at the sole discretion of the Development Code Administrator.

28. **Effective Date.** The Effective Date of this Agreement shall be the day this Agreement is recorded in the Public Records of Volusia County, Florida.

Attachment: Development Agreement (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

IN WITNESS WHEREOF, the Owners, the Developer and the City have executed this Agreement.

OWNER: KBL PROPERTY INVESTMENTS, LLC

By:

_____
Signature of Witness # 1

_____
Signature

_____
Print or type name

_____
Print or type name

As:

_____
Signature of Witness #2

_____
Print or type

ATTEST:

_____
Print or type name

_____
Signature

_____
Print or Type Name

STATE OF FLORIDA
COUNTY OF _____

The foregoing instrument was acknowledged before me, **by means of ☐ physical presence or ☐ online notarization,** this ____ day of _____, _____ (year), by _____, who is _____ of KBL Property Investments, LLC, and who is ___ personally known to me or ___ produced _____ as identification.

NOTARY PUBLIC, STATE OF FLORIDA

_____
Notary Signature

_____
Printed Name

Commission No.: _____
My Commission Expires: _____

Attachment: Development Agreement (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

OWNER: CHARLESDALE ASSOCIATES, INC.

By:

_____
Signature of Witness # 1

_____
Signature

_____
Print or type name

_____
Print or type name
As:

_____
Signature of Witness #2

_____
Print or type

ATTEST:

_____
Print or type name

_____
Signature

_____
Print or Type Name

STATE OF FLORIDA
COUNTY OF _____

The foregoing instrument was acknowledged before me, **by means of ☐ physical presence or ☐ online notarization,** this ____ day of _____, _____ (year), by _____, who is _____ of Charlesdale Associates, Inc. and who is ___ personally known to me or ___ produced _____ as identification.

NOTARY PUBLIC, STATE OF FLORIDA

_____
Notary Signature

_____
Printed Name

Commission No.: _____
My Commission Expires: _____

Attachment: Development Agreement (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

DEVELOPER: STEIN INVESTMENT CO, LLC

By:

_____
Signature of Witness # 1

_____
Signature

_____
Print or type name

_____
Print or type name
As:

_____
Signature of Witness #2

_____
Print or type

_____
Print or type name

ATTEST:

_____
Signature

_____
Print or Type Name

STATE OF FLORIDA
COUNTY OF _____

The foregoing instrument was acknowledged before me, **by means of ☐ physical presence or ☐ online notarization,** this ____ day of _____, _____ (year), by _____, who is _____ of Stein Investment Co, LLC. and who is ____ personally known to me or ___ produced _____ as identification.

NOTARY PUBLIC, STATE OF FLORIDA

_____
Notary Signature

_____
Printed Name

Commission No.: _____
My Commission Expires: _____

Attachment: Development Agreement (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

CITY OF HOLLY HILL:

By: _____

Date: _____

ATTEST:

_____

Date: _____

Mailing Address:
City of Holly Hill
1065 Ridgewood Ave.
Holly Hill, Florida 32117

STATE OF FLORIDA
COUNTY OF _____

The foregoing instrument was acknowledged before me, **by means of ☐ physical presence or ☐ online notarization,** this ____ day of _____, _____ (year), by _____, who is personally known to me or produced _____ as identification.

NOTARY PUBLIC, STATE OF FLORIDA

_____
Notary Signature

_____
Printed Name

Commission No.: _____
My Commission Expires: _____

Approved as to form and legality for use and reliance by the City of Holly Hill, Florida

_____
Scott Simpson, City Attorney

Attachment: Development Agreement (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

EXHIBIT "A"
Legal Description

PARCEL A:

LOT 5, BRITTON'S SUBDIVISION, ACCORDING TO THE PLAT THEREOF RECORDED IN MAP BOOK 9, PAGE 143, OF THE PUBLIC RECORDS OF VOLUSIA COUNTY, FLORIDA. LESS AND EXCEPT ANY PORTION LYING WITH THE STATE ROAD RIGHT OF WAY.

LOTS 4 AND 6, BRITTON SUBDIVISION, AS RECORDED IN PLAT AS RECORDED IN MAP BOOK 9, PAGE 143, OF THE PUBLIC RECORDS OF VOLUSIA COUNTY, FLORIDA. LESS AND EXCEPT ANY PORTION LYING WITHIN THE STATE ROAD RIGHT OF WAY.
LOTS 7 AND 8, BRITTON SUBDIVISION, AS RECORDED IN PLAT AS RECORDED IN MAP BOOK 9 PAGE 143, OF THE PUBLIC RECORDS OF VOLUSIA COUNTY, FLORIDA.
LOT 1, AND WESTERLY 24.9 FEET OF LOT 2, BLOCK A, SAULSBURY PLACE, ACCORDING TO THE MAP OR PLAT THEREOF AS RECORDED IN PLAT BOOK 6, PAGE 103, OF THE PUBLIC RECORDS OF VOLUSIA COUNTY, FLORIDA.
LOT 2, EXCEPT THE EAST 25.3 FEET AND THE WEST 24.9 FEET BLOCK A, SAULSBURY PLACE, ACCORDING TO THE MAP OR PLAT THEREOF AS RECORDED IN PLAT BOOK 6, PAGE 103, OF THE PUBLIC RECORDS OF VOLUSIA COUNTY, FLORIDA.

PARCEL B:

PARCEL 1:
LOT 6, EXCEPTING THE WESTERLY 9.0 FEET THEREOF AND EXCEPTING THE WESTERLY 30 FEET OF THE NORTHERLY 60.7 FEET THEREOF, SIMPSON SUBDIVISION AS PER MAP IN MAP BOOK 11, PAGE 131, AND EXCEPTING THAT PORTION DEEDED FOR STATE ROAD RIGHT OF WAY BEING MORE PARTICULARLY DESCRIBED IN WARRANTY DEED RECORDED OFFICIAL RECORDS BOOK 3899, PAGE 2533, OF THE PUBLIC RECORDS OF VOLUSIA COUNTY, FLORIDA.

PARCEL 2:
PART OF LOT ONE (1), SIMPSON'S SUBDIVISION, BEING A RESUBDIVISION OF A PORTION OF BLOCK THIRTY-SIX (36), MASON AND CARSWELL'S HOLLY HILL, FLORIDA, AS PER MAP RECORDED IN MAP BOOK 11, PAGE 131, OF THE PUBLIC RECORDS OF VOLUSIA COUNTY, FLORIDA, DESCRIBED AS FOLLOWS: BEGINNING AT A POINT ON THE NORTHERLY RIGHT-OF-WAY LINE OF MASON AVENUE (60 FEET WIDE) AT THE DISTANCE OF 158.78 FEET MEASURED ALONG SAID RIGHT-OF-WAY LINE OF MASON AVENUE SOUTH 63 DEGREES 27 MINUTES 46 SECONDS WEST FROM THE SOUTHERLY END OF THE CURVED LINE WHICH CONNECTS THE NORTHERLY RIGHT-OF-WAY LINE OF MASON AVENUE WITH THE WESTERLY RIGHT-OF-WAY LINE OF NORTH BEACH STREET (ALSO KNOWN AS DIXIE HIGHWAY), SAID POINT OF BEGINNING ALSO BEING AT THE SOUTHWESTERLY CORNER OF PREMISES CONVEYED BY THE ATLANTIC REFINING COMPANY TO METROPOLITAN LIFE INSURANCE COMPANY, BY DEED DATED DECEMBER 15, 1952, AND RECORDED AMONG THE PUBLIC RECORDS OF VOLUSIA COUNTY, IN DEED BOOK 479, PAGE 202; FROM SAID POINT OF BEGINNING EXTENDING THENCE (1) ALONG SAID RIGHT-OF-WAY LINE OF MASON AVENUE, SOUTH 63 DEGREES 27 MINUTES 46 SECONDS WEST 138.88 FEET TO A POINT IN LINE OF OTHER LANDS CONVEYED BY THE ATLANTIC REFINING COMPANY TO

Attachment: Development Agreement (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

R. C. WILLIAMS, THENCE (2) ALONG SAID OTHER LANDS CONVEYED BY THE ATLANTIC REFINING COMPANY TO R. C. WILLIAMS, NORTH 26 DEGREES 32 MINUTES 14 SECONDS WEST 197.67 FEET TO A POINT ON THE SOUTHERLY RIGHT-OF-WAY LINE OF RIVERSIDE PLACE; THENCE (3) ALONG SAID SOUTHERLY RIGHT-OF-WAY OF RIVERSIDE PLACE, NORTH 63 DEGREES 24 MINUTES EAST 138.87 FEET TO A POINT IN LINE OF OTHER LANDS OF THE ATLANTIC REFINING COMPANY; AND THENCE (4) PARTLY ALONG LINE OF OTHER LANDS OF THE ATLANTIC REFINING COMPANY AND PARTLY ALONG LINE OF LANDS OF METROPOLITAN LIFE INSURANCE COMPANY, SOUTH 26 DEGREES 32 MINUTES 14 SECONDS EAST 197.83 FEET TO THE PLACE OF BEGINNING.

ALSO, BEGINNING AT A POINT ON THE NORTHERLY RIGHT-OF-WAY LINE OF MASON AVENUE (60 FEET WIDE) THE DISTANCE OF 297.66 FEET MEASURED ALONG SAID RIGHT-OF-WAY LINE OF MASON AVENUE SOUTH 63 DEGREES 27 MINUTES 46 SECONDS WEST FROM THE SOUTHERLY END OF THE CURVED LINE WHICH CONNECTS THE NORTHERLY RIGHT-OF-WAY LINE OF MASON AVENUE WITH THE WESTERLY RIGHT-OF-WAY LINE OF NORTH BEACH STREET (ALSO KNOWN AS DIXIE HIGHWAY), SAID POINT OF BEGINNING ALSO BEING AT THE SOUTHWESTERLY CORNER OF OTHER LANDS CONVEYED BY THE ATLANTIC REFINING COMPANY TO R. C. WILLIAMS; FROM SAID POINT OF BEGINNING EXTENDING THENCE (1) ALONG SAID RIGHT-OF-WAY LINE OF MASON AVENUE SOUTH 63 DEGREES 27 MINUTES 46 SECONDS WEST 150 FEET TO A POINT AT THE SOUTHWESTERLY CORNER OF SAID LOT NO. 1 OF "THE SIMPSON SUBDIVISION"; THENCE (2) ALONG THE WESTERLY LINE OF SAID LOT NO. 1 NORTH 26 DEGREES 30 MINUTES WEST 197.50 FEET TO A POINT ON THE SOUTHERLY RIGHT-OF-WAY LINE OF RIVERSIDE PLACE AT THE NORTHWESTERLY CORNER OF SAID LOT NO. 1, THENCE (3) ALONG SAID SOUTHERLY RIGHT-OF-WAY LINE OF RIVERSIDE PLACE, NORTH 63 DEGREES 24 MINUTES EAST 149.87 FEET TO A POINT IN LINE OF SAID OTHER LANDS CONVEYED BY THE ATLANTIC REFINING COMPANY TO R. C. WILLIAMS, AND THENCE (4) ALONG SAID LINE OF OTHER LANDS CONVEYED TO R. C. WILLIAMS SOUTH 26 DEGREES 32 MINUTES 14 SECONDS EAST 197.67 FEET TO THE PLACE OF BEGINNING.

EXCEPTING FROM THE ABOVE-DESCRIBED PARCEL, THAT PORTION DEEDED FOR STATE ROAD RIGHT-OF-WAY BEING MORE PARTICULARLY DESCRIBED IN WARRANTY DEED RECORDED IN OFFICIAL RECORDS BOOK 3899. PAGE 2533, OF THE PUBLIC RECORDS OF VOLUSIA COUNTY, FLORIDA.

PARCEL C:

PARCEL 1:
THE EASTERLY 25.3 FEET OF LOT TWO (2) AND THE WESTERLY 25 FEET OF LOT THREE (3), AS MEASURED ALONG FIRST STREET, BLOCK "A", SAULSBURY'S PLACE, A SUBDIVISION OF BLOCK 36, MASON AND CARSWELL'S HOLLY HILL, AS PER MAP THEREOF IN MAP BOOK 6, PAGE 103, OF THE PUBLIC RECORDS OF VOLUSIA COUNTY, FLORIDA.

AND

THE EAST 3/4 OF LOT 3, BLOCK "A", SAULSBURY PLACE, HOLLY HILL, AND INCLUDING WEST 30 FEET OF NORTH 60 FEET OF LOT 6, SIMPSON SUBDIVISION, BLOCK 36, MASON AND CARSWELL'S HOLLY HILL AS PER MAP THEREOF IN MAP BOOK 11, PAGE 131, OF THE

Attachment: Development Agreement (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

PUBLIC RECORDS OF VOLUSIA COUNTY, FLORIDA.

AND

PARCEL 2:
LOT TWO (2), BRITTON SUBDIVISION, PER MAP IN MAP BOOK 9, PAGE 143, OF THE PUBLIC RECORDS OF VOLUSIA COUNTY, FLORIDA, AND ALSO THE WESTERLY 9 FEET OF LOT ELEVEN (11), AND THE WESTERLY 9 FEET OF THE SOUTH 1/2 OF LOT TWELVE (12), BLOCK 36, MASON AND CARSWELL'S HOLLY HILL, PER MAP RECORDED IN MAP BOOK 2, PAGE 90, OF THE PUBLIC RECORDS OF VOLUSIA COUNTY, FLORIDA, AND LOT THREE (3), BRITTON'S SUBDIVISION OF THE SOUTH 1/2 OF LOT NINE (9), AND ALL OF LOT TEN (10), BLOCK 36, MASON AND CARSWELL'S HOLLY HILL, ACCORDING TO THE MAP RECORDED IN BOOK 9, PAGE 143, OF THE PUBLIC RECORDS OF VOLUSIA COUNTY, FLORIDA.

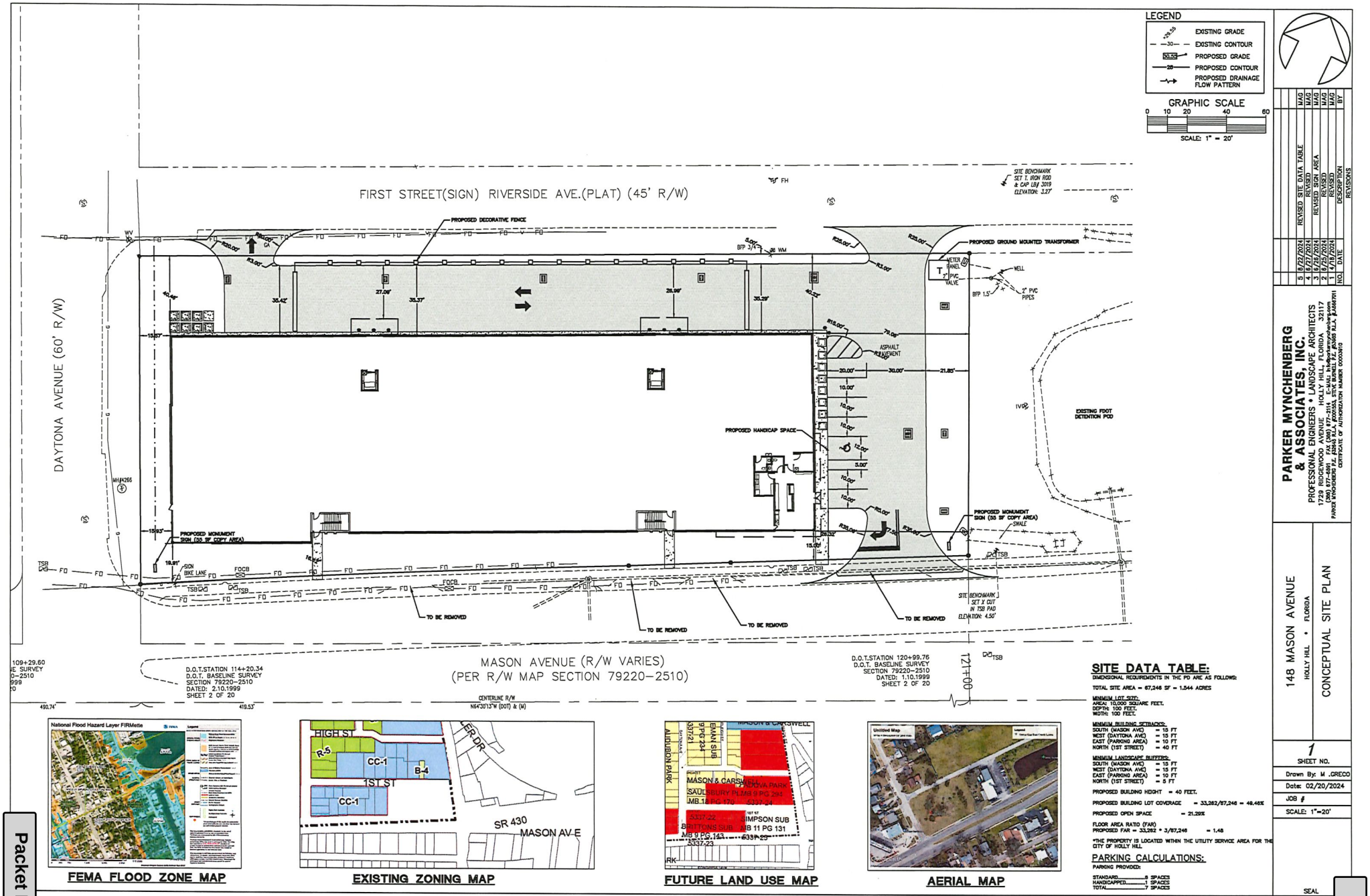
LESS AND EXCEPT THAT PORTION TAKEN BY ORDER OF TAKING RECORDED APRIL 25, 1994 IN OFFICIAL RECORDS BOOK 3914, PAGE 427, OF THE PUBLIC RECORDS OF VOLUSIA COUNTY, FLORIDA, DESCRIBED AS FOLLOWS:

THAT PART OF LOTS 2 AND 3, BRITTON'S SUBDIVISION, AS RECORDED IN MAP BOOK 9, PAGE 143, AND LOT 6, THE SIMPSON SUBDIVISION, AS RECORDED IN MAP BOOK 11, PAGE 131, OF THE PUBLIC RECORDS OF VOLUSIA COUNTY, FLORIDA IN SECTION 37, TOWNSHIP 15 SOUTH, RANGE 33 EAST, DESCRIBED AS FOLLOWS:
COMMENCE AT THE 3" IRON PIPE MARKING THE NORTHWEST CORNER OF LOT 8, OF SAID BRITTON'S SUBDIVISION; THENCE SOUTH 25°20'46" EAST, ALONG THE EAST LINE OF DAYTONA AVENUE, 136.53 FEET TO THE SOUTHWEST CORNER OF LOT 6, OF SAID BRITTON'S SUBDIVISION; THENCE NORTH 64°29'54" EAST ALONG THE EXISTING NORTHERLY RIGHT-OF-WAY LINE OF STATE ROAD 430, A DISTANCE OF 200.00 FEET TO THE SOUTHWEST CORNER OF LOT 3, OF SAID BRITTON'S SUBDIVISION FOR THE POINT OF BEGINNING; THENCE NORTH 25°20'46" WEST ALONG THE WEST LINE OF SAID LOT 3, A DISTANCE OF 37.71 FEET TO A POINT OF INTERSECTION WITH A NON-TANGENT CURVE, CONCAVE SOUTHEASTERLY, HAVING A RADIUS OF 7,685.56 FEET, AND A CHORD BEARING NORTH 63°13'46" EAST; THENCE NORTHEASTERLY ALONG THE ARC OF SAID CURVE THROUGH A CENTRAL ANGLE OF 00°21'14", A DISTANCE OF 47.47 FEET TO A POINT OF REVERSE CURVATURE WITH A CURVE, CONCAVE NORTHWESTERLY, HAVING A RADIUS OF 11,414.38 FEET, AND A CHORD BEARING NORTH 63°16'40" EAST; THENCE NORTHEASTERLY ALONG THE ARC OF SAID CURVE THROUGH A CENTRAL ANGLE OF 00°15'32", A DISTANCE OF 51.56 FEET TO THE POINT OF INTERSECTION WITH THE EAST LINE OF THE WEST 9.00 FEET OF LOT 6, OF SAID THE SIMPSON SUBDIVISION; THENCE SOUTH 25°20'46" EAST ALONG SAID EAST LINE, 39.86 FEET TO THE EXISTING NORTHERLY RIGHT-OF-WAY LINE OF STATE ROAD 430; THENCE SOUTH 64°29'54" WEST ALONG SAID EXISTING NORTHERLY RIGHT-OF-WAY LINE, 99.00 FEET, TO THE POINT OF BEGINNING.

Attachment: Development Agreement (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

EXHIBIT "B"
Preliminary Plan

Attachment: Development Agreement (2024-O-3079 : Mason Avenue Storage Facility Planned Development)



FEMA FLOOD ZONE MAP

EXISTING ZONING MAP

FUTURE LAND USE MAP

AERIAL MAP

SITE DATA TABLE:

DIMENSIONAL REQUIREMENTS IN THE PD ARE AS FOLLOWS:

TOTAL SITE AREA = 67,246 SF = 1.544 ACRES

MINIMUM LOT SIZE:
AREA: 10,000 SQUARE FEET.
DEPTH: 100 FEET.
WIDTH: 100 FEET.

MINIMUM BUILDING SETBACKS:
SOUTH (MASON AVE) = 15 FT
WEST (DAYTONA AVE) = 15 FT
EAST (PARKING AREA) = 10 FT
NORTH (1ST STREET) = 40 FT

MINIMUM LANDSCAPE BUFFERS:
SOUTH (MASON AVE) = 15 FT
WEST (DAYTONA AVE) = 15 FT
EAST (PARKING AREA) = 10 FT
NORTH (1ST STREET) = 5 FT

PROPOSED BUILDING HEIGHT = 40 FEET.

PROPOSED BUILDING LOT COVERAGE = 33,282/67,246 = 49.48%

PROPOSED OPEN SPACE = 21.29%

FLOOR AREA RATIO (FAR)
PROPOSED FAR = 33,282 ÷ 3/67,246 = 1.48

*THE PROPERTY IS LOCATED WITHIN THE UTILITY SERVICE AREA FOR THE CITY OF HOLLY HILL

PARKING CALCULATIONS:

PARKING PROVIDED:

STANDARD.....6 SPACES
HANDICAPPED.....1 SPACES
TOTAL.....7 SPACES

NO.	DATE	DESCRIPTION	BY
		REVISIONS	
5	8/22/2024	REVISED SITE DATA TABLE	MAG
4	8/07/2024	REVISED	MAG
3	6/28/2024	REVISED SIGN AREA	MAG
2	5/25/2024	REVISED	MAG
1	4/18/2024	REVISED	MAG

PARKER MYNCHENBERG & ASSOCIATES, INC.
PROFESSIONAL ENGINEERS • LANDSCAPE ARCHITECTS
1729 RIDGEWOOD AVENUE HOLLY HILL, FLORIDA 32117
(386) 677-6168 FAX (386) 677-8165
PARKER MYNCHENBERG P.E. #39416 R.L.A. #0001554, STEVE BURNELL P.E. #59685 R.L.A. #6666701
CERTIFICATE OF AUTHORIZATION NUMBER 00003910

148 MASON AVENUE
HOLLY HILL • FLORIDA

CONCEPTUAL SITE PLAN

1
SHEET NO.

Drawn By: M .CRECO
Date: 02/20/2024
JOB #
SCALE: 1"=20'

SEAL

Attachment: Development Agreement (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

ALTA / NSPS LAND TITLE SURVEY

FOR

STEIN INVESTMENT COMPANY, LLC.

A PORTION OF

SECTION 37–TOWNSHIP 15 SOUTH–RANGE 33 EAST
VOLUSIA COUNTY, FLORIDA

LOCATION

134 MASON AVENUE, HOLLY HILL, FLORIDA

LEGAL DESCRIPTION: (PROVIDED BY CLIENT)

PARCEL A:

LOT 5, BRITTON'S SUBDIVISION, ACCORDING TO THE PLAT THEREOF RECORDED IN MAP BOOK 9, PAGE 143, OF THE PUBLIC RECORDS OF VOLUSIA COUNTY, FLORIDA. LESS AND EXCEPT ANY PORTION LYING WITH THE STATE ROAD RIGHT OF WAY.

LOTS 4 AND 6, BRITTON SUBDIVISION, AS RECORDED IN PLAT AS RECORDED IN MAP BOOK 9, PAGE 143, OF THE PUBLIC RECORDS OF VOLUSIA COUNTY, FLORIDA. LESS AND EXCEPT ANY PORTION LYING WITHIN THE STATE ROAD RIGHT OF WAY.

LOTS 7 AND 8, BRITTON SUBDIVISION, AS RECORDED IN PLAT AS RECORDED IN MAP BOOK 9 PAGE 143, OF THE PUBLIC RECORDS OF VOLUSIA COUNTY, FLORIDA.

LOT 1, AND WESTERLY 24.9 FEET OF LOT 2, BLOCK A, SAULSBURY PLACE, ACCORDING TO THE MAP OR PLAT THEREOF AS RECORDED IN PLAT BOOK 6, PAGE 103, OF THE PUBLIC RECORDS OF VOLUSIA COUNTY, FLORIDA.

LOT 2, EXCEPT THE EAST 25.3 FEET AND THE WEST 24.9 FEET BLOCK A, SAULSBURY PLACE, ACCORDING TO THE MAP OR PLAT THEREOF AS RECORDED IN PLAT BOOK 6, PAGE 103, OF THE PUBLIC RECORDS OF VOLUSIA COUNTY, FLORIDA.

PARCEL B:

PARCEL 1

LOT 6, EXCEPTING THE WESTERLY 9.0 FEET THEREOF AND EXCEPTING THE WESTERLY 30 FEET OF THE NORTHERLY 60.7 FEET THEREOF, SIMPSON SUBDIVISION AS PER MAP IN MAP BOOK 11, PAGE 131, AND EXCEPTING THAT PORTION DEEDED FOR STATE ROAD RIGHT OF WAY BEING MORE PARTICULARLY DESCRIBED IN WARRANTY DEED RECORDED OFFICIAL RECORDS BOOK 3899, PAGE 2533, OF THE PUBLIC RECORDS OF VOLUSIA COUNTY, FLORIDA.

PARCEL 2

PART OF LOT ONE (1), SIMPSON'S SUBDIVISION, BEING A RESUBDIVISION OF A PORTION OF BLOCK THIRTY–SIX (36), MASON AND CARSWELL'S HOLLY HILL, FLORIDA, AS PER MAP RECORDED IN MAP BOOK 11, PAGE 131, OF THE PUBLIC RECORDS OF VOLUSIA COUNTY, FLORIDA, DESCRIBED AS FOLLOWS: BEGINNING AT A POINT ON THE NORTHERLY RIGHT–OF–WAY LINE OF MASON AVENUE (60 FEET WIDE) AT THE DISTANCE OF 158.78 FEET MEASURED ALONG SAID RIGHT–OF–WAY LINE OF MASON AVENUE SOUTH 63 DEGREES 27 MINUTES 46 SECONDS WEST FROM THE SOUTHERLY END OF THE CURVED LINE WHICH CONNECTS THE NORTHERLY RIGHT–OF–WAY LINE OF MASON AVENUE WITH THE WESTERLY RIGHT–OF–WAY LINE OF NORTH BEACH STREET (ALSO KNOWN AS DIXIE HIGHWAY), SAID POINT OF BEGINNING ALSO BEING AT THE SOUTHWESTERLY CORNER OF PREMISES CONVEYED BY THE ATLANTIC REFINING COMPANY TO METROPOLITAN LIFE INSURANCE COMPANY, BY DEED DATED DECEMBER 15, 1952, AND RECORDED AMONG THE PUBLIC RECORDS OF VOLUSIA COUNTY, IN DEED BOOK 479, PAGE 202; FROM SAID POINT OF BEGINNING EXTENDING THENCE (1) ALONG SAID RIGHT–OF–WAY LINE OF MASON AVENUE, SOUTH 63 DEGREES 27 MINUTES 46 SECONDS WEST 138.88 FEET TO A POINT IN LINE OF OTHER LANDS CONVEYED BY THE ATLANTIC REFINING COMPANY TO R. C. WILLIAMS, THENCE (2) ALONG SAID OTHER LANDS CONVEYED BY THE ATLANTIC REFINING COMPANY TO R. C. WILLIAMS, NORTH 26 DEGREES 32 MINUTES 14 SECONDS WEST 197.67 FEET TO A POINT ON THE SOUTHERLY RIGHT–OF–WAY LINE OF RIVERSIDE PLACE; THENCE (3) ALONG SAID SOUTHERLY RIGHT–OF–WAY LINE OF RIVERSIDE PLACE, NORTH 63 DEGREES 24 MINUTES EAST 138.87 FEET TO A POINT IN LINE OF OTHER LANDS OF THE ATLANTIC REFINING COMPANY; AND THENCE (4) PARTLY ALONG LINE OF OTHER LANDS OF THE ATLANTIC REFINING COMPANY AND PARTLY ALONG LINE OF LANDS OF METROPOLITAN LIFE INSURANCE COMPANY, SOUTH 26 DEGREES 32 MINUTES 14 SECONDS EAST 197.83 FEET TO THE PLACE OF BEGINNING.

ALSO, BEGINNING AT A POINT ON THE NORTHERLY RIGHT–OF–WAY LINE OF MASON AVENUE (60 FEET WIDE) THE DISTANCE OF 297.66 FEET MEASURED ALONG SAID RIGHT–OF–WAY LINE OF MASON AVENUE SOUTH 63 DEGREES 27 MINUTES 46 SECONDS WEST FROM THE SOUTHERLY END OF THE CURVED LINE WHICH CONNECTS THE NORTHERLY RIGHT–OF–WAY LINE OF MASON AVENUE WITH THE WESTERLY RIGHT–OF–WAY LINE OF NORTH BEACH STREET (ALSO KNOWN AS DIXIE HIGHWAY), SAID POINT OF BEGINNING ALSO BEING AT THE SOUTHWESTERLY CORNER OF OTHER LANDS CONVEYED BY THE ATLANTIC REFINING COMPANY TO R. C. WILLIAMS; FROM SAID POINT OF BEGINNING EXTENDING THENCE (1) ALONG SAID RIGHT–OF–WAY LINE OF MASON AVENUE SOUTH 63 DEGREES 27 MINUTES 46 SECONDS WEST 150 FEET TO A POINT AT THE SOUTHWESTERLY CORNER OF SAID LOT NO. 1 OF "THE SIMPSON SUBDIVISION"; THENCE (2) ALONG THE WESTERLY LINE OF SAID LOT NO. 1 NORTH 26 DEGREES 30 MINUTES WEST 197.50 FEET TO A POINT ON THE SOUTHERLY RIGHT–OF–WAY LINE OF RIVERSIDE PLACE AT THE NORTHWESTERLY CORNER OF SAID LOT NO. 1, THENCE (3) ALONG SAID SOUTHERLY RIGHT–OF–WAY LINE OF RIVERSIDE PLACE, NORTH 63 DEGREES 24 MINUTES EAST 149.87 FEET TO A POINT IN LINE OF SAID OTHER LANDS CONVEYED BY THE ATLANTIC REFINING COMPANY TO R. C. WILLIAMS, AND THENCE (4) ALONG SAID LINE OF OTHER LANDS CONVEYED TO R. C. WILLIAMS SOUTH 26 DEGREES 32 MINUTES 14 SECONDS EAST 197.67 FEET TO THE PLACE OF BEGINNING.

EXCEPTING FROM THE ABOVE DESCRIBED PARCEL, THAT PORTION DEEDED FOR STATE ROAD RIGHT–OF–WAY BEING MORE PARTICULARLY DESCRIBED IN WARRANTY DEED RECORDED IN OFFICIAL RECORDS BOOK 3899. PAGE 2533, OF THE PUBLIC RECORDS OF VOLUSIA COUNTY, FLORIDA.

PARCEL C:

PARCEL 1:

THE EASTERLY 25.3 FEET OF LOT TWO (2) AND THE WESTERLY 25 FEET OF LOT THREE (3), AS MEASURED ALONG FIRST STREET, BLOCK "A", SAULSBURY'S PLACE, A SUBDIVISION OF BLOCK 36, MASON AND CARSWELL'S HOLLY HILL, AS PER MAP THEREOF IN MAP BOOK 6, PAGE 103, OF THE PUBLIC RECORDS OF VOLUSIA COUNTY, FLORIDA.

AND

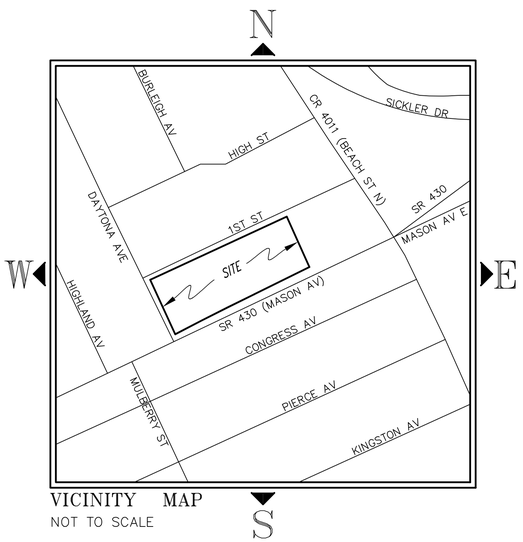
THE EAST 3/4 OF LOT 3, BLOCK "A", SAULSBURY PLACE, HOLLY HILL, AND INCLUDING WEST 30 FEET OF NORTH 60 FEET OF LOT 6, SIMPSON SUBDIVISION, BLOCK 36, MASON AND CARSWELL'S HOLLY HILL AS PER MAP THEREOF IN MAP BOOK 11, PAGE 131, OF THE PUBLIC RECORDS OF VOLUSIA COUNTY, FLORIDA.

AND

CONTINUED...

ZONING INFORMATION

NONE PROVIDED.



VICINITY MAP
NOT TO SCALE

LEGAL DESCRIPTION CONTINUED:

PARCEL 2:

LOT TWO (2), BRITTON SUBDIVISION, PER MAP IN MAP BOOK 9, PAGE 143, OF THE PUBLIC RECORDS OF VOLUSIA COUNTY, FLORIDA, AND ALSO THE WESTERLY 9 FEET OF LOT ELEVEN (11), AND THE WESTERLY 9 FEET OF THE SOUTH 1/2 OF LOT TWELVE (12), BLOCK 36, MASON AND CARSWELL'S HOLLY HILL, PER MAP RECORDED IN MAP BOOK 2, PAGE 90, OF THE PUBLIC RECORDS OF VOLUSIA COUNTY, FLORIDA, AND LOT THREE (3), BRITTON'S SUBDIVISION OF THE SOUTH 1/2 OF LOT NINE (9), AND ALL OF LOT TEN (10), BLOCK 36, MASON AND CARSWELL'S HOLLY HILL, ACCORDING TO THE MAP RECORDED IN BOOK 9, PAGE 143, OF THE PUBLIC RECORDS OF VOLUSIA COUNTY, FLORIDA.

LESS AND EXCEPT THAT PORTION TAKEN BY ORDER OF TAKING RECORDED APRIL 25, 1994 IN OFFICIAL RECORDS BOOK 3914, PAGE 427, OF THE PUBLIC RECORDS OF VOLUSIA COUNTY, FLORIDA, DESCRIBED AS FOLLOWS:

THAT PART OF LOTS 2 AND 3, BRITTON'S SUBDIVISION, AS RECORDED IN MAP BOOK 9, PAGE 143, AND LOT 6, THE SIMPSON SUBDIVISION, AS RECORDED IN MAP BOOK 11, PAGE 131, OF THE PUBLIC RECORDS OF VOLUSIA COUNTY, FLORIDA IN SECTION 37, TOWNSHIP 15 SOUTH, RANGE 33 EAST, DESCRIBED AS FOLLOWS:

COMMENCE AT THE 3" IRON PIPE MARKING THE NORTHWEST CORNER OF LOT 8, OF SAID BRITTON'S SUBDIVISION; THENCE SOUTH 25°20'46" EAST, ALONG THE EAST LINE OF DAYTONA AVENUE, 136.53 FEET TO THE SOUTHWEST CORNER OF LOT 6, OF SAID BRITTON'S SUBDIVISION; THENCE NORTH 64°29'54" EAST ALONG THE EXISTING NORTHERLY RIGHT–OF–WAY LINE OF STATE ROAD 430, A DISTANCE OF 200.00 FEET TO THE SOUTHWEST CORNER OF LOT 3, OF SAID BRITTON'S SUBDIVISION FOR THE POINT OF BEGINNING; THENCE NORTH 25°20'46" WEST ALONG THE WEST LINE OF SAID LOT 3, A DISTANCE OF 37.71 FEET TO A POINT OF INTERSECTION WITH A NON–TANGENT CURVE, CONCAVE SOUTHEASTERLY, HAVING A RADIUS OF 7,685.56 FEET, AND A CHORD BEARING NORTH 63°13'46" EAST; THENCE NORTHEASTERLY ALONG THE ARC OF SAID CURVE THROUGH A CENTRAL ANGLE OF 00°21'14", A DISTANCE OF 47.47 FEET TO A POINT OF REVERSE CURVATURE WITH A CURVE, CONCAVE NORTHWESTERLY, HAVING A RADIUS OF 11,414.38 FEET, AND A CHORD BEARING NORTH 63°16'40" EAST; THENCE NORTHEASTERLY ALONG THE ARC OF SAID CURVE THROUGH A CENTRAL ANGLE OF 00°15'32", A DISTANCE OF 51.56 FEET TO THE POINT OF INTERSECTION WITH THE EAST LINE OF THE WEST 9.00 FEET OF LOT 6, OF SAID THE SIMPSON SUBDIVISION; THENCE SOUTH 25°20'46" EAST ALONG SAID EAST LINE, 39.86 FEET TO THE EXISTING NORTHERLY RIGHT–OF–WAY LINE OF STATE ROAD 430; THENCE SOUTH 64°29'54" WEST ALONG SAID EXISTING NORTHERLY RIGHT–OF–WAY LINE, 99.00 FEET, TO THE POINT OF BEGINNING.

INDEX OF SHEETS:

1 COVER SHEET (CURRENT)

2 ALTA/NSPS LAND TITLE SURVEY

NOTE:
THIS SURVEY IS NOT VALID WITHOUT SHEETS 1 TO 2

SURVEY NOTES:

1. THIS PLAT OF SURVEY HAS BEEN PREPARED WITH THE BENEFIT OF A TITLE COMMITMENT PREPARED BY FIDELITY NATIONAL TITLE INSURANCE COMPANY, HAVING A COMMITMENT NUMBER OF FL252312090JC/232691ATL, AND DATED DECEMBER 26, 2023, AT 08:00 AM.

2. THE MEASURED BEARINGS SHOWN HEREON ARE (GRID BEARINGS) BASED ON THE FLORIDA STATE PLANE COORDINATE SYSTEM, EAST ZONE, 1983 NORTH AMERICAN DATUM, 2007 ADJUSTMENT, DERIVING A BEARING OF N25° 19' 41"W, ALONG EASTERLY RIGHT OF WAY OF DAYTONA AVENUE.

3. UNDERGROUND FOUNDATIONS, IF ANY HAVE NOT BEEN LOCATED OR SHOWN AS A PART OF THIS SURVEY.

4. EVIDENCE OF ABOVE GROUND UTILITIES HAVE BEEN LOCATED AS A PART OF THIS SURVEY. UNDERGROUND UTILITIES HAVE BEEN LOCATED BY SLIGER AND ASSOCIATES, INC. AS MARKED BY "CALL SUNSHINE", 811.

5. ELEVATIONS REFER TO N.A.V.D. OF 1988, PER THE CITY OF DAYTONA BEACH PUBLIC WORKS DEPARTMENT, ENGINEERING DIVISION BENCHMARK NUMBER RMR–17 HAVING A PUBLISHED ELEVATION OF 3.293 FEET.

6. THIS PROPERTY IS LOCATED IN FLOOD INSURANCE RATE MAP (F.I.R.M.) ZONE "X". THIS LOCATION IS DETERMINED BY SCALING FROM F.I.R.M. MAP NO. 12127C0357 J. MAP EFFECTIVE DATE: SEPT. 29, 2017. APPROXIMATE SCALE: 1"= 500'.

7. UNLESS OTHERWISE SHOWN, RECORDING INFORMATION IS FROM THE PUBLIC RECORDS OF VOLUSIA COUNTY.

8. DISTANCES ARE IN FEET AND DECIMALS THEREOF.

ADDITIONAL SURVEY NOTES:

A. THERE ARE INTERNAL OVERLAPS BASED ON THE LEGAL DESCRIPTION AS PROVIDED. THERE ARE NO GAPS, GORES, OVERLAPS OR HIATUS INHERENT TO THE SURVEYED OVERALL EXTERIOR BOUNDARY. THIS SURVEYOR RECOMMENDS A NEW DESCRIPTION AND SURVEYORS AFFIDAVIT BE COMPLETED TO REPLACE THIS LONG AND COMPLICATED DESCRIPTION.

B. THE SURVEYED PROPERTY HAS DIRECT ACCESS TO MASON AVENUE, DAYTONA AVENUE AND RIVERSIDE AVENUE (1ST STREET).

C. THERE IS NO OBSERVABLE EVIDENCE OF CEMETERIES, BURIAL GROUNDS, OR INDIVIDUAL GRAVESITES.

D. THIS SURVEYOR IS NOT QUALIFIED TO MAKE WETLAND DETERMINATIONS, AND DID NOT OBSERVE ANY MARKINGS PLACED BY ANY BIOLOGIST ON THE SURVEYED PROPERTIES WITH REGARDS TO WETLANDS.

E. THERE ARE NO DIVISION OR PARTY WALLS DESIGNATED BY THE CLIENT OR LOCATED BY THE SURVEYOR WITH RESPECT TO ADJOINING PROPERTIES.

F. NO OFFSITE EASEMENTS OR SERVITUDE BENEFITTING THE SURVEYED PROPERTIES WERE DISCLOSED IN THE RECORD DOCUMENTS PROVIDED TO THE SURVEYOR OR OBSERVED IN THE PROCESS OF CONDUCTING THE SURVEY.

G. AT THE TIME OF SURVEY, THE SURVEYOR WAS NOT AWARE OF ANY PROPOSED CHANGES IN THE STREET RIGHT OF WAY LINES OR OBSERVABLE EVIDENCE OF STREET OR SIDEWALK REPAIRS.

H. THE SUBJECT PROPERTY DOES NOT CONTAIN ANY VISIBLE EVIDENCE OF SITE USE AS A SOLID WASTE DUMP, SUMP OR SANITARY LANDFILL.

I. NOTE THAT THE TITLE LINES AND ACTUAL POSSESSION LINES ARE THE SAME.

SCHEDULE B, PART II – EXCEPTIONS

SOME HISTORICAL LAND RECORDS CONTAIN DISCRIMINATORY COVENANTS THAT ARE ILLEGAL AND UNENFORCEABLE BY LAW. THIS COMMITMENT AND THE POLICY TREAT ANY DISCRIMINATORY COVENANT IN A DOCUMENT REFERENCED IN SCHEDULE B AS IF EACH DISCRIMINATORY COVENANT IS REDACTED, REPUDIATED, REMOVED, AND NOT REPUBLISHED OR RECIRCULATED. ONLY THE REMAINING PROVISIONS OF THE DOCUMENT WILL BE EXCEPTED FROM COVERAGE.
THE POLICY WILL NOT INSURE AGAINST LOSS OR DAMAGE RESULTING FROM THE TERMS AND CONDITIONS OF ANY LEASE OR EASEMENT IDENTIFIED IN SCHEDULE A, AND WILL INCLUDE THE FOLLOWING EXCEPTIONS UNLESS CLEARED TO THE SATISFACTION OF THE COMPANY:

1. ANY DEFECT, LIEN, ENCUMBRANCE, ADVERSE CLAIM, OR OTHER MATTER THAT APPEARS FOR THE FIRST TIME IN THE PUBLIC RECORDS OR IS CREATED, ATTACHES, OR IS DISCLOSED BETWEEN THE COMMITMENT DATE AND THE DATE ON WHICH ALL OF THE SCHEDULE B, PART I—REQUIREMENTS ARE MET.

2. TAXES AND ASSESSMENTS FOR THE YEAR 2024 AND SUBSEQUENT YEARS, WHICH ARE NOT YET DUE AND PAYABLE.

3. ANY LIEN, OR RIGHT TO A LIEN, FOR SERVICES, LABOR, OR MATERIALS HERETOFORE OR HEREAFTER FURNISHED, IMPOSED BY LAW, AND NOT SHOWN BY THE PUBLIC RECORDS.

4. INTENTIONALLY DELETED.

5. RIGHTS OR CLAIMS OF PARTIES IN POSSESSION NOT SHOWN BY THE PUBLIC RECORDS.

6. UNPAID CHARGES FOR PUBLIC UTILITIES FURNISHED BY ANY COUNTY, MUNICIPALITY, OR PUBLIC SERVICE CORPORATION, WHICH MAY BE OR MAY BECOME A LIEN UPON THE LAND INSURED HEREBY UNDER ANY PROVISION OF THE FLORIDA STATUTES, INCLUDING SECTION 159.17, AND/OR ANY COUNTY, MUNICIPAL, OR SPECIAL TAXING DISTRICT ASSESSMENT, INCLUDING THOSE LEVIED UNDER THE PROVISIONS OF CHAPTER 190, FLORIDA STATUTES.
ITEMS #1–6 ARE STANDARD EXCEPTIONS.

7. RESERVATIONS IN FAVOR OF THE STATE OF FLORIDA AS SET FORTH IN THE DEED BOOK 315, PAGE 263. HOWEVER THE RIGHT OF ENTRY AND EXPLORATION ASSOCIATED WITH THE OIL AND MINERAL RESERVATION HAS BEEN RELEASED PURSUANT TO SECTION 270.11. F.S.
NOT A SURVEY MATTER.

8. MATTERS AS SHOWN ON THE SURVEY BY SLIGER & ASSOCIATES, INC. DATED FEBRUARY 21, 2024, LAST REVISED _____, 2024, UNDER JOB NO. 24–0153, PROJECT NO. 08716, AS FOLLOWS:

a) 2 OVERHEAD POWER LINES AND A POWER POLE ENCROACH INTO THE SUBJECT PROPERTY ALONG NORTH BOUNDARY.
b) 2 UNDERGROUND SEWER LINES AND A CLEAN OUT ENCROACH ONTO THE SUBJECT PROPERTY ALONG THE NORTHERLY BOUNDARY
c) UNDERGROUND FIBER OPTIC CABLE LINE AND FIBER OPTIC CABLE BOX ENCROACH ONTO THE SUBJECT PROPERTY ALONG THE SOUTHWEST CORNER/ SOUTHERLY BOUNDARY
d) SIGN FOR BIKE LANE ENCROACHES INTO THE SUBJECT PROPERTY ALONG THE SOUTHWEST CORNER

ALL SHOWN HEREON.

SURVEYOR'S REPORT:

PURPOSE OF SURVEY:

PREPARE AN ALTA / NSPS LAND TITLE SURVEY AS DIRECTED BY THE CLIENT & FOR THE CLIENTS USE.
ADDRESSES INCLUDE:
120, 134, 140 & 148 MASON AVENUE, HOLLY HILL, FLORIDA.
105 DAYTONA AVENUE, HOLLY HILL, FLORIDA.
145, 149, 151 & 155 1ST STREET, HOLLY HILL, FLORIDA.

METHODOLOGY:

HORIZONTAL DATUM – NORTH AMERICAN 1983. COORDINATES – STATE PLANE, FLORIDA EAST ZONE.
HORIZONTAL CONTROL POINT RMR 17, HAVING PUBLISHED COORDINATES OF NORTH 1,780,211.953 AND EAST 647,115.933 WAS OCCUPIED USING GLOBAL POSITIONING SATELLITE RECEIVER, AND ON SITE SECONDARY CONTROL WAS ESTABLISHED. THEN, CONVENTIONAL TOTAL STATION SURVEYING TECHNIQUES USED FOR LOCATIONS.

VERTICAL DATUM – NORTH AMERICAN 1988.
REFERENCE BENCHMARK RECOVERED 4"X4" CONCRETE MONUMENT WITH 3" BRASS DISC IN CENTER, STAMPED "CONTROL MONUMENT RMR–17". PUBLISHED ELEVATION 3.293 FEET.

ON SITE VERTICAL CONTROL WAS ESTABLISHED BY A 3 WIRE LEVEL LOOP THROUGH THE HORIZONTAL CONTROL ESTABLISHED HEREON.

ERROR OF CLOSURE

HORIZONTAL ERROR OF CLOSURE:
THE PREDICTED RELATIVE POSITIONAL ACCURACY FOR THE GLOBAL POSITIONING AND CONVENTIONAL TOTAL STATION EQUIPMENT USED TO PREFORM THIS SURVEY DOES NOT EXCEED 0.07 FEET PLUS 50 PARTS PER MILLION HORIZONTAL AND WAS VERIFIED BY REDUNDANT FIELD OBSERVATIONS.

ADJUSTMENT METHOD:
A STATISTICALLY SIGNIFICANT PORTION OF THE FIELD DATA WAS VERIFIED BY REDUNDANT GPS OBSERVATIONS AS MEETING THE ABOVE MENTIONED POSITIONAL TOLERANCE AND NOT ADJUSTED.

VERTICAL ERROR OF CLOSURE:
ON SITE VERTICAL CONTROL WAS ESTABLISHED BY A 3 WIRE LEVEL LOOP THROUGH THE HORIZONTAL CONTROL ESTABLISHED HEREON WITH AN ERROR OF CLOSURE OF 1: 20,000.

REFERENCE MATERIAL:

NATIONAL GEODETIC DATABASE
THE CITY OF DAYTONA BEACH PUBLIC WORKS DEPARTMENT – ENGINEERING DIVISION DATABASE
F.E.M.A. ONLINE FLOOD MAP SERVICE CENTER
VOLUSIA COUNTY PROPERTY APPRAISER WEBSITE
FLORIDA DEPARTMENT OF TRANSPORTATION RIGHT OF WAY MAP OF STATE ROAD 430,SECTION 79220–2510 SHEETS 2 & 14 OF 20, DATED 7/2/1993.
SURVEY BY SLIGER & ASSOCIATES, INC. JOB No. 22–0962, DATED JULY 18, 2022
INFORMATION PROVIDED WITHIN FIDELITY NATION TITLE INSURANCE COMPANY COMMITMENT FOR TITLE INSURANCE, COMMITMENT NUMBER: FL252312090JC/232691ATL, DATED DECEMBER 26, 2023 AT 08:00 AM.

UTILITY CONTACTS:

THE UNDERGROUND UTILITIES SHOWN HAVE BEEN LOCATED FROM FIELD INFORMATION AND EXISTING DRAWINGS. THE SURVEYOR MAKES NO GUARANTEES THAT THE UNDERGROUND UTILITIES SHOWN COMPRISE ALL SUCH UTILITIES IN THE AREA, EITHER IN–SERVICE OR ABANDONED. THE SURVEYOR FURTHER DOES NOT WARRANT THAT THE UNDERGROUND UTILITIES SHOWN ARE IN THE EXACT LOCATION INDICATED ALTHOUGH THE SURVEYOR DOES CERTIFY THAT THEY ARE LOCATED AS ACCURATELY AS POSSIBLE FROM THE INFORMATION AVAILABLE. THE SURVEYOR HAS NOT PHYSICALLY LOCATED THE UNDERGROUND UTILITIES.

UTILITY COMPANIES HAVE BEEN CONTACTED THROUGH "CALL SUNSHINE" (UNDERGROUND CABLE LOCATING SERVICE) 1–800–432–4770 TICKET NO. 045400754, 045400811 & 045400821 AS PER THE "UNDERGROUND FACILITY DAMAGE PREVENTION ACT".

THE FOLLOWING UTILITIES RESPONDED AFTER NOTIFICATION BY "CALL SUNSHINE".

PEOPLES GAS SYSTEM – MARKED

CHARTER–TIME WARNER CABLE – NOT MARKED

FLORIDA POWER & LIGHT – NOT MARKED

UNITI FIBER – NOT MARKED

CITY OF HOLLY HILL – MARKED

WIRE 3, LLC – MARKED

HOTWIRE COMMUNICATIONS – NOT MARKED

METRO FIBERNET LLC – NOT MARKED

NOTICE:

THIS SURVEY IS NOT VALID WITHOUT THE SIGNATURE AND THE ORIGINAL RAISED SEAL OR A VALID ELECTRONIC SIGNATURE OF A FLORIDA LICENSED SURVEYOR AND MAPPER.

SURVEYOR'S CERTIFICATION:

TO: FIDELITY NATIONAL TITLE INSURANCE COMPANY, STEIN INVESTMENT COMPANY, LLC., KBL PROPERTY INVESTMENTS, LLC & CHARLESDALE ASSOCIATES, INC.

THIS IS TO CERTIFY THAT THIS MAP OR PLAT AND THE SURVEY ON WHICH IT IS BASED WERE MADE IN ACCORDANCE WITH THE 2016 MINIMUM STANDARD DETAIL REQUIREMENTS FOR ALTA/NSPS LAND TITLE SURVEYS, JOINTLY ESTABLISHED AND ADOPTED BY ALTA AND NSPS, AND INCLUDES ITEMS 1, 2, 3, 4, 6(a), 6(b), 7(a), 7(b)(1), 7(c), 8, 9, 11(a), 11(b), 13, 16, 17, 18 & 19 OF TABLE A THEREOF.
THE FIELDWORK WAS COMPLETED ON FEBRUARY 21, 2024.
DATE OF PLAT OR MAP: MARCH 12, 2024 (SURVEYOR'S SIGNATURE, PRINTED)

Jeffrey S Hattendorf
Digitally signed by Jeffrey S Hattendorf
Date: 2024.03.14 07:47:22 -04'00'
DATE:

JEFFREY HATTENDORF
PROFESSIONAL SURVEYOR AND MAPPER
FLORIDA LICENSE NUMBER 6193

SLIGER & ASSOCIATES, INC.
PROFESSIONAL LAND SURVEYORS
3921 NOVA ROAD
PORT ORANGE, FL. 32127
(386) 756-0908
LICENSED BUSINESS CERTIFICATION NUMBER 3019
Copyright © 2024 Sliger & Associates, Inc.

No.	Date	Revision
1		
2		
3		
4		
5		

FIELD BOOK:1527
PAGE (S): 35–39
FIELD DATE: FEB. 21, 2024
PARTY CHIEF: S. STRICKLAND
DRAWN BY: IDV
CHECKED BY: J. HATTENDORF

ALTA / NSPS LAND TITLE SURVEY
134 MASON AVENUE
HOLLY HILL, FLORIDA
CLIENT: STEIN INVESTMENT COMPANY, LLC.

PROJECT: 08716
JOB: 24–0153
SCALE: N/A
SHEET: 1 OF 2

FILE: K:\24\240153 148 MASON\240153–IDV.DWG

Attachment: Exhibit A - Legal & Survey (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

ABBREVIATIONS:

W/	WITH	ILLEG.	ILLEGIBLE	GLM	GAS LINE MARKER	LB	LICENSED BUSINESS	LP	LIGHT POLE
IRC	IRON ROD & CAP	MB	MAP BOOK	D	CENTRAL ANGLE	DIP	DUCTILE IRON PIPE	PP	POWER POLE
IR	IRON ROD (NO CAP)	PG	PAGE	R	RADIUS	PVC	POLYVINYL CHLORIDE	GA	GUY ANCHOR
IPC	IRON PIPE & CAP	ORB	OFFICIAL RECORDS BOOK	L	ARC LENGTH	CONC	CONCRETE	TSP	TRAFFIC SIGNAL POLE
IP	IRON PIPE (NO CAP)	(P)	PLATTED DIMENSION	CB	CHORD BEARING	RES	RESIDENCE	R/W	RIGHT OF WAY
CM	CONCRETE MONUMENT	(D)	DEED DIMENSION	CH	CHORD DISTANCE	CO	CLEANOUT	DW	DRIVEWAY
N&D	NAIL & DISK	(M)	MEASURED DIMENSION	SAN	SANITARY	ES	ELECTRIC SERVICE	TOB	TOP OF BANK
FND	FOUND	(C)	CALCULATED DIMENSION	MH	MANHOLE	CV	CHECK VALVE	TOE	TOE OF SLOPE
MW	MONITORING WELL	(R)	RADIAL	MES	MITERED END SECTION	IV	IRRIGATION VALVE	CLS	CENTERLINE OF SWALE
ID	IDENTIFICATION	(NR)	NON RADIAL	HDPE	HIGH DENSITY POLYETHYLENE PIPE	WV	WATER VALVE	A/C	AIR CONDITIONER
(TYP)	TYPICAL	STA	STATION	RCP	REINFORCED CONCRETE PIPE	RV	REUSE VALVE	FNC	FENCE
SEC	SECTION	EL	ELEVATION	CMP	CORRUGATED METAL PIPE	WM	WATER METER	EOW	EDGE OF WATER
TWP	TOWNSHIP	INV	INVERT	CPP	CORRUGATED PLASTIC PIPE	FH	FIRE HYDRANT	U.E.	UTILITY EASEMENT
RGE	RANGE	℄	CENTERLINE	VCP	VITREOUS CLAY PIPE	TC	TOP COVER	A.E.	ACCESS EASEMENT

−FO−	BURIED FIBER OPTIC CABLE	FP&L CO	FLORIDA POWER & LIGHT COMPANY
−T−	BURIED TELEPHONE CABLE	NGVD	NATIONAL GEODETIC VERTICAL DATUM
−W−	BURIED WATER LINE	NAVD	NORTH AMERICAN VERTICAL DATUM
−E−	BURIED ELECTRIC LINE	FDOT	FLORIDA DEPARTMENT OF TRANSPORTATION
−G−	BURIED GAS LINE	FDNR	FLORIDA DEPARTMENT OF NATURAL RESOURCES
−TV−	BURIED TELEVISION LINE	USC & GS	UNITED STATES COAST & GEODETIC SURVEY
−FM−	BURIED FORCEMAIN		
−OH−	AERIAL UTILITY LINE		
−ST−	STORM WATER LINE		

LEGEND:

●	IRON ROD WITH CAP	⊗ GV	GAS VALVE	⊠ FOCB	FIBER OPTIC CABLE BOX
○	IRON ROD	⊗ RUV	REUSE VALVE	⊠ FOCV	FIBER OPTIC CABLE VAULT
◉	IRON PIPE WITH CAP	⊗ SSV	SANITARY SEWER VALVE	ELP	ELECTRIC PANEL
◎	IRON PIPE	⊗ HHE	HAND HOLE (ELECTRIC)	FOCM	FIBER OPTIC CABLE MARKER
○	NAIL & DISK	⊠ WM	WATER METER	TPM	TELEPHONE CABLE MARKER
⊛	FD "X"/CUT IN CONCRETE	⊠ GM	GAS METER		SIGN
□	CONCRETE MONUMENT	⊠ TB	TELEPHONE BOX	LP	LIGHT POLE
△	DENOTES PC / PT	⊠ MB	MAIL BOX	YL	YARD LIGHT
■	PERMANENT CONTROL POINT	◪ TV	CABLE TELEVISION BOX		UTILITY POLE
◔	SITE BENCHMARK	TSB	TRAFFIC SIGNAL BOX	GA	GUY ANCHOR
FH	FIRE HYDRANT	⊗ WV	WATER VALVE	EB	ELECTRIC SERVICE BOX
—	CHANGE OF DIRECTION				

Ⓢ	SSMH	SANITARY SEWER MANHOLE	
Ⓓ	SDMH	STORM DRAIN MANHOLE	
Ⓖ	GTMH	GREASE TRAP MANHOLE	
Ⓔ	EMH	ELECTRIC MANHOLE	
Ⓤ	UMH	UTILITY MANHOLE	
◎	CO	CLEAN OUT	
Ⓕ	FOC	FIBER OPTIC CABLE MANHOLE	
⋈	RBO	REUSE BLOWOFF ASSEMBLY	
▲		WETLANDS LOCATION	
▨		EXISTING CONCRETE	
0.00 ×		EXISTING ELEVATION	

GRAPHIC SCALE
0 20 40
SCALE: 1" = 20'

SANITARY MH#4196
TOP=3.75'
E.INV.=-1.45' 8" CLAY
W.INV.=0.00' 8" CLAY
SW. INV.=-0.51 6" CLAY

SANITARY MH#4232
TOP=12.40'
N.INV.=6.00 8" CLAY
S.INV.=3.70' 8" CLAY
E.INV.=4.40' 8" CLAY

SANITARY MH#4328
TOP=2.81'
E.INV.=-1.99 8" CLAY
W.INV.=-1.96' 8" CLAY

SANITARY MH#4259
TOP=11.58'
N.INV.=5.12 8" CLAY

STORM MH#4429
TOP=5.10'
E.INV.=0.90' 24" RCP
W.INV.=0.66' 18" RCP
S.INV.=0.72' 18" RCP
W.INV.=2.40' 8"" CPP

STORM MH#4183
TOP=4.48'
N.INV.=-1.82' 24" RCP
S.INV.=-0.05' 18" RCP
E.INV.=-0.77' 24" RCP
W.INV.=-1.32'

STORM INLET#4180
TOP=2.83'
(INACCESSIBLE)

STORM MH#46010
TOP=4.05'
E.INV.=-0.60' 30" RCP
NW.INV.=-0.60' 30" RCP

STORM INLET#4569
TOP=3.36'
E.INV.=-0.32' 15" RCP
SE.INV.=-0.25' 36" RCP
N.INV.=1.50' 4" PVC

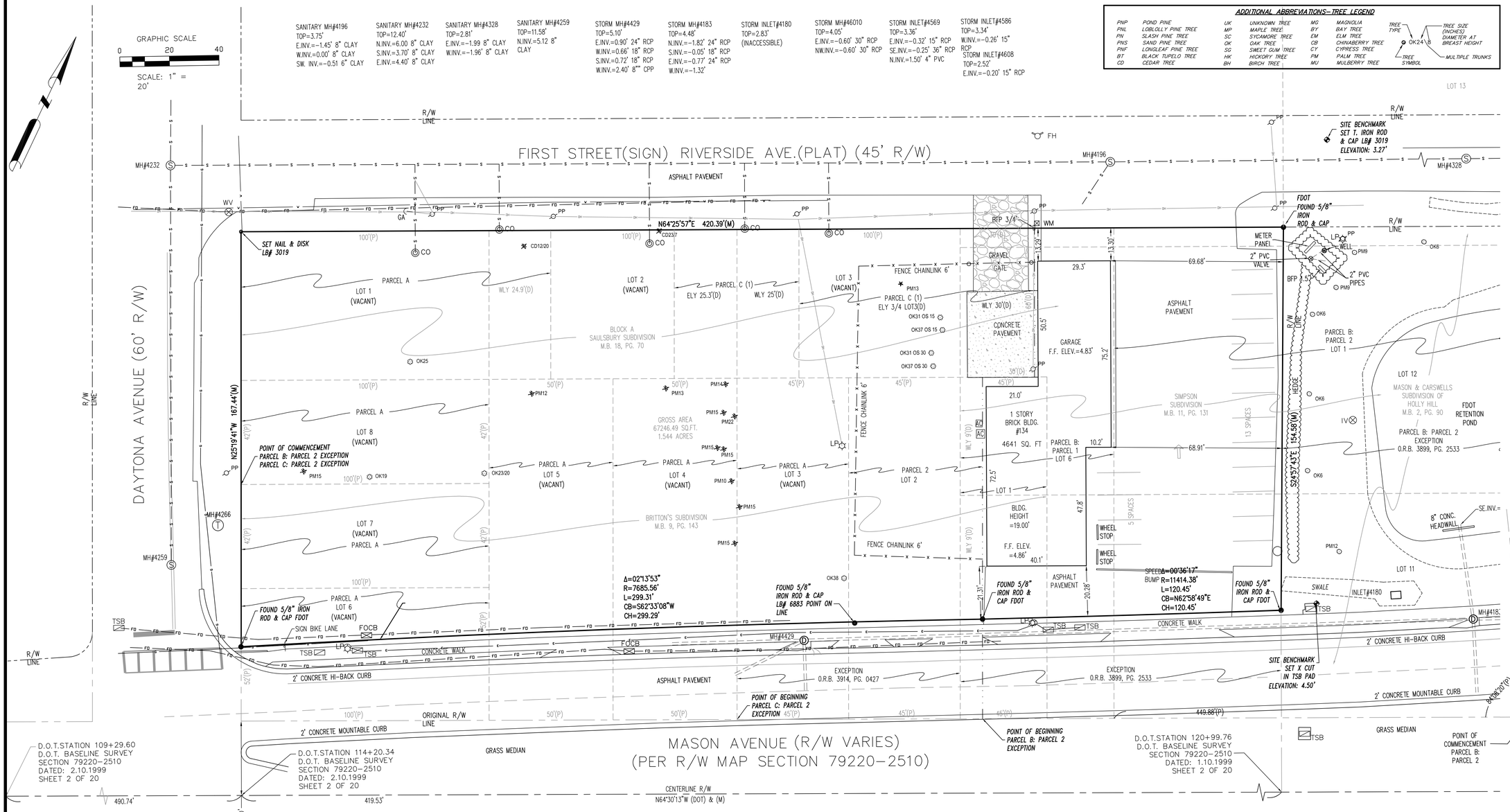
STORM INLET#4586
TOP=3.34'
W.INV.=-0.26' 15" RCP

STORM INLET#4608
TOP=2.52'
E.INV.=-0.20' 15" RCP

ADDITIONAL ABBREVIATIONS-TREE LEGEND

PNP	POND PINE	UK	UNKNOWN TREE	MG	MAGNOLIA
PNL	LOBLOLLY PINE TREE	MP	MAPLE TREE	BY	BAY TREE
PN	SLASH PINE TREE	SC	SYCAMORE TREE	EM	ELM TREE
PNS	SAND PINE TREE	OK	OAK TREE	CB	CHINABERRY TREE
PNF	LONGLEAF PINE TREE	SG	SWEET GUM TREE	CY	CYPRESS TREE
BT	BLACK TUPELO TREE	HK	HICKORY TREE	PM	PALM TREE
CD	CEDAR TREE	BH	BIRCH TREE	MU	MULBERRY TREE

TREE TYPE — OK24 — 8 — TREE SIZE (INCHES) DIAMETER AT BREAST HEIGHT
TREE SYMBOL — MULTIPLE TRUNKS



NOTE:
THIS SURVEY IS NOT VALID WITHOUT SHEETS 1 TO 2

SEE SHEET 1 OF 2 FOR:
SURVEYORS NOTES
BOUNDARY DESCRIPTION

SLIGER & ASSOCIATES, INC.
PROFESSIONAL LAND SURVEYORS
3921 NOVA ROAD
PORT ORANGE, FL 32127
(386) 788-7822
LICENSED BUSINESS CERTIFICATION NUMBER 3019
Copyright © 2023 Sliger & Associates, Inc.

No.	Date	Revision	Approved
1			
2			
3			
4			
5			

ALTA / NSPS LAND TITLE SURVEY
134 MASON AVENUE
HOLLY HILL, FLORIDA
CLIENT: STEIN INVESTMENT COMPANY, LLC.

FIELD DATE: FEB. 21, 2024
PARTY CHIEF: S. STRICKLAND
DRAWN BY: IDV
CHECKED BY: J. HATTENDORF
FIELD BOOK: 1527
PAGE (S): 35-39

PROJECT: 08716
JOB: 24-0153
SCALE: 1" = 20'
SHEET: 2 OF 2

FILE: K:\24\240153 148 MASON\240153-IDV.DWG

Attachment: Exhibit A - Legal & Survey (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

VOLUSIA COUNTY PROPERTY APPRAISER
LARRY BARTLETT, JD, CFA
WE VALUE VOLUSIA

Volusia County Property Appraiser
123 W. Indiana Ave., Rm. 102
DeLand, FL. 32720
Phone: (386) 736-5901 Web: vcpa.vcgov.org

AltKey: 3473876 **Parcel ID: 533722010021**
CHARLESDALE ASSOCIATES INC **145 1ST ST, HOLLY HILL, FL**

Parcel Summary

Alternate Key:	3473876
Parcel ID:	533722010021
Township-Range-Section:	15 - 33 - 37
Subdivision-Block-Lot:	22 - 01 - 0021
Owner(s):	CHARLESDALE ASSOCIATES INC - FS - Fee Simple - 100%
Mailing Address On File:	134 MASON AVE DAYTONA BEACH FL 32117
Physical Address:	145 1ST ST, HOLLY HILL 32117
Property Use:	1000 - VACANT COMM
Tax District:	203-HOLLY HILL
2023 Final Millage Rate:	18.223
Neighborhood:	7230
Subdivision Name:	
Homestead Property:	No

Attachment: Exhibit B1 - Charlesdale Assoc, Inc (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

VOLUSIA COUNTY PROPERTY APPRAISER
LARRY BARTLETT, JD, CFA
WE VALUE VOLUSIA

Volusia County Property Appraiser
123 W. Indiana Ave., Rm. 102
DeLand, FL. 32720
Phone: (386) 736-5901 Web: vcpa.vcgov.org

AltKey: 3473931 **Parcel ID: 533723000020**
CHARLESDALE ASSOCIATES INC **140 MASON AVE, HOLLY HILL, FL**

Parcel Summary

Alternate Key:	3473931
Parcel ID:	533723000020
Township-Range-Section:	15 - 33 - 37
Subdivision-Block-Lot:	23 - 00 - 0020
Owner(s):	CHARLESDALE ASSOCIATES INC - FS - Fee Simple - 100%
Mailing Address On File:	134 MASON AVE DAYTONA BEACH FL 32117
Physical Address:	140 MASON AVE, HOLLY HILL 32117
Property Use:	1000 - VACANT COMM
Tax District:	203-HOLLY HILL
2023 Final Millage Rate:	18.223
Neighborhood:	7230
Subdivision Name:	BRITTONS
Homestead Property:	No

Attachment: Exhibit B1 - Charlesdale Assoc, Inc (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

VOLUSIA COUNTY PROPERTY APPRAISER
LARRY BARTLETT, JD, CFA
WE VALUE VOLUSIA

Volusia County Property Appraiser
123 W. Indiana Ave., Rm. 102
DeLand, FL. 32720
Phone: (386) 736-5901 Web: vcpa.vcgov.org

AltKey: 3474147 **Parcel ID: 533725000060**
CHARLESDALE ASSOCIATES INC **134 MASON AVE, HOLLY HILL, FL**

Parcel Summary

Alternate Key:	3474147
Parcel ID:	533725000060
Township-Range-Section:	15 - 33 - 37
Subdivision-Block-Lot:	25 - 00 - 0060
Owner(s):	CHARLESDALE ASSOCIATES INC - FS - Fee Simple - 100%
Mailing Address On File:	134 MASON AVE HOLLY HILL FL 32117
Physical Address:	134 MASON AVE, HOLLY HILL 32117
Property Use:	2700 - AUTO SALES
Tax District:	203-HOLLY HILL
2023 Final Millage Rate:	18.223
Neighborhood:	7230
Subdivision Name:	SIMPSONS
Homestead Property:	No

Attachment: Exhibit B1 - Charlesdale Assoc, Inc (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

VOLUSIA COUNTY PROPERTY APPRAISER
LARRY BARTLETT, JD, CFA
WE VALUE VOLUSIA

Volusia County Property Appraiser
123 W. Indiana Ave., Rm. 102
DeLand, FL. 32720
Phone: (386) 736-5901 Web: vcpa.vcgov.org

AltKey: 3474104 **Parcel ID: 533725000011**
CHARLESDALE ASSOCIATES INC **120 MASON AVE, HOLLY HILL, FL**

Parcel Summary

Alternate Key:	3474104
Parcel ID:	533725000011
Township-Range-Section:	15 - 33 - 37
Subdivision-Block-Lot:	25 - 00 - 0011
Owner(s):	CHARLESDALE ASSOCIATES INC - FS - Fee Simple - 100%
Mailing Address On File:	134 MASON AVE HOLLY HILL FL 32117
Physical Address:	120 MASON AVE, HOLLY HILL 32117
Property Use:	1000 - VACANT COMM
Tax District:	203-HOLLY HILL
2023 Final Millage Rate:	18.223
Neighborhood:	7230
Subdivision Name:	SIMPSONS
Homestead Property:	No

Attachment: Exhibit B1 - Charlesdale Assoc, Inc (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

VOLUSIA COUNTY PROPERTY APPRAISER
LARRY BARTLETT, JD, CFA
WE VALUE VOLUSIA

Volusia County Property Appraiser
123 W. Indiana Ave., Rm. 102
DeLand, FL. 32720
Phone: (386) 736-5901 Web: vcpa.vcgov.org

AltKey: 5439011 **Parcel ID: 533723000041**
KBL PROPERTY INVESTMENTS LLC **MASON AVE, HOLLY HILL, FL**

Parcel Summary

Alternate Key:	5439011
Parcel ID:	533723000041
Township-Range-Section:	15 - 33 - 37
Subdivision-Block-Lot:	23 - 00 - 0041
Owner(s):	KBL PROPERTY INVESTMENTS LLC - FS - Fee Simple - 100%
Mailing Address On File:	PO BOX 148
	FLAGLER BEACH FL 32136
Physical Address:	MASON AVE, HOLLY HILL 32117
Property Use:	1000 - VACANT COMM
Tax District:	203-HOLLY HILL
2023 Final Millage Rate:	18.223
Neighborhood:	7230
Subdivision Name:	BRITTONS
Homestead Property:	No

Attachment: Exhibit B2 - KBL Property Investments, LLC (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

VOLUSIA COUNTY PROPERTY APPRAISER
LARRY BARTLETT, JD, CFA
WE VALUE VOLUSIA

Volusia County Property Appraiser
123 W. Indiana Ave., Rm. 102
DeLand, FL. 32720
Phone: (386) 736-5901 Web: vcpa.vcgov.org

AltKey: 3473957 **Parcel ID: 533723000050**
KBL PROPERTY INVESTMENTS LLC **148 MASON AVE, HOLLY HILL, FL**

Parcel Summary

Alternate Key:	3473957
Parcel ID:	533723000050
Township-Range-Section:	15 - 33 - 37
Subdivision-Block-Lot:	23 - 00 - 0050
Owner(s):	KBL PROPERTY INVESTMENTS LLC - FS - Fee Simple - 100%
Mailing Address On File:	PO BOX 148
	FLAGLER BEACH FL 32136
Physical Address:	148 MASON AVE, HOLLY HILL 32117
Property Use:	1000 - VACANT COMM
Tax District:	203-HOLLY HILL
2023 Final Millage Rate:	18.223
Neighborhood:	7230
Subdivision Name:	BRITTONS
Homestead Property:	No

Attachment: Exhibit B2 - KBL Property Investments, LLC (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

VOLUSIA COUNTY PROPERTY APPRAISER
LARRY BARTLETT, JD, CFA
WE VALUE VOLUSIA

Volusia County Property Appraiser
123 W. Indiana Ave., Rm. 102
DeLand, FL. 32720
Phone: (386) 736-5901 Web: vcpa.vcgov.org

AltKey: 5439071 **Parcel ID: 533723000061**
KBL PROPERTY INVESTMENTS LLC **DAYTONA AVE, HOLLY HILL, FL**

Parcel Summary

Alternate Key:	5439071
Parcel ID:	533723000061
Township-Range-Section:	15 - 33 - 37
Subdivision-Block-Lot:	23 - 00 - 0061
Owner(s):	KBL PROPERTY INVESTMENTS LLC - FS - Fee Simple - 100%
Mailing Address On File:	PO BOX 148
	FLAGLER BEACH FL 32136
Physical Address:	DAYTONA AVE, HOLLY HILL 32117
Property Use:	1000 - VACANT COMM
Tax District:	203-HOLLY HILL
2023 Final Millage Rate:	18.223
Neighborhood:	7230
Subdivision Name:	BRITTONS
Homestead Property:	No

Attachment: Exhibit B2 - KBL Property Investments, LLC (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

VOLUSIA COUNTY PROPERTY APPRAISER
LARRY BARTLETT, JD, CFA
WE VALUE VOLUSIA

Volusia County Property Appraiser
123 W. Indiana Ave., Rm. 102
DeLand, FL. 32720
Phone: (386) 736-5901 Web: vcpa.vcgov.org

AltKey: 3473973 **Parcel ID: 533723000070**
KBL PROPERTY INVESTMENTS LLC **105 DAYTONA AVE, HOLLY HILL, FL**

Parcel Summary

Alternate Key:	3473973
Parcel ID:	533723000070
Township-Range-Section:	15 - 33 - 37
Subdivision-Block-Lot:	23 - 00 - 0070
Owner(s):	KBL PROPERTY INVESTMENTS LLC - FS - Fee Simple - 100%
Mailing Address On File:	PO BOX 148
	FLAGLER BEACH FL 32136
Physical Address:	105 DAYTONA AVE, HOLLY HILL 32117
Property Use:	1000 - VACANT COMM
Tax District:	203-HOLLY HILL
2023 Final Millage Rate:	18.223
Neighborhood:	7230
Subdivision Name:	BRITTONS
Homestead Property:	No

Attachment: Exhibit B2 - KBL Property Investments, LLC (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

VOLUSIA COUNTY PROPERTY APPRAISER
LARRY BARTLETT, JD, CFA
WE VALUE VOLUSIA

Volusia County Property Appraiser
123 W. Indiana Ave., Rm. 102
DeLand, FL. 32720
Phone: (386) 736-5901 Web: vcpa.vcgov.org

AltKey: 3473981 **Parcel ID: 533723000080**
KBL PROPERTY INVESTMENTS LLC **148 MASON AVE, DAYTONA BEACH, FL**

Parcel Summary

Alternate Key:	3473981
Parcel ID:	533723000080
Township-Range-Section:	15 - 33 - 37
Subdivision-Block-Lot:	23 - 00 - 0080
Owner(s):	KBL PROPERTY INVESTMENTS LLC - FS - Fee Simple - 100%
Mailing Address On File:	PO BOX 148
	FLAGLER BEACH FL 32136
Physical Address:	148 MASON AVE, DAYTONA BEACH 32117
Property Use:	1000 - VACANT COMM
Tax District:	203-HOLLY HILL
2023 Final Millage Rate:	18.223
Neighborhood:	7230
Subdivision Name:	BRITTONS
Homestead Property:	No

Attachment: Exhibit B2 - KBL Property Investments, LLC (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

VOLUSIA COUNTY PROPERTY APPRAISER
LARRY BARTLETT, JD, CFA
WE VALUE VOLUSIA

Volusia County Property Appraiser
123 W. Indiana Ave., Rm. 102
DeLand, FL. 32720
Phone: (386) 736-5901 Web: vcpa.vcgov.org

AltKey: 3473841 **Parcel ID: 533722010010**
KBL PROPERTY INVESTMENTS LLC **155 1ST ST, HOLLY HILL, FL**

Parcel Summary

Alternate Key:	3473841
Parcel ID:	533722010010
Township-Range-Section:	15 - 33 - 37
Subdivision-Block-Lot:	22 - 01 - 0010
Owner(s):	KBL PROPERTY INVESTMENTS LLC - FS - Fee Simple - 100%
Mailing Address On File:	PO BOX 148
	FLAGLER BEACH FL 32136
Physical Address:	155 1ST ST, HOLLY HILL 32117
Property Use:	1000 - VACANT COMM
Tax District:	203-HOLLY HILL
2023 Final Millage Rate:	18.223
Neighborhood:	7230
Subdivision Name:	
Homestead Property:	No

Attachment: Exhibit B2 - KBL Property Investments, LLC (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

VOLUSIA COUNTY PROPERTY APPRAISER
LARRY BARTLETT, JD, CFA
WE VALUE VOLUSIA

Volusia County Property Appraiser
123 W. Indiana Ave., Rm. 102
DeLand, FL. 32720
Phone: (386) 736-5901 Web: vcpa.vcgov.org

AltKey: 3473850 **Parcel ID: 533722010011**
KBL PROPERTY INVESTMENTS LLC **151 1ST ST, HOLLY HILL, FL**

Parcel Summary

Alternate Key:	3473850
Parcel ID:	533722010011
Township-Range-Section:	15 - 33 - 37
Subdivision-Block-Lot:	22 - 01 - 0011
Owner(s):	KBL PROPERTY INVESTMENTS LLC - FS - Fee Simple - 100%
Mailing Address On File:	PO BOX 148
	FLAGLER BEACH FL 32136
Physical Address:	151 1ST ST, HOLLY HILL 32117
Property Use:	1000 - VACANT COMM
Tax District:	203-HOLLY HILL
2023 Final Millage Rate:	18.223
Neighborhood:	7230
Subdivision Name:	
Homestead Property:	No

Attachment: Exhibit B2 - KBL Property Investments, LLC (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

VOLUSIA COUNTY PROPERTY APPRAISER
LARRY BARTLETT, JD, CFA
WE VALUE VOLUSIA

Volusia County Property Appraiser
123 W. Indiana Ave., Rm. 102
DeLand, FL. 32720
Phone: (386) 736-5901 Web: vcpa.vcgov.org

AltKey: 3473868 **Parcel ID: 533722010020**
KBL PROPERTY INVESTMENTS LLC **149 1ST ST, HOLLY HILL, FL**

Parcel Summary

Alternate Key:	3473868
Parcel ID:	533722010020
Township-Range-Section:	15 - 33 - 37
Subdivision-Block-Lot:	22 - 01 - 0020
Owner(s):	KBL PROPERTY INVESTMENTS LLC - FS - Fee Simple - 100%
Mailing Address On File:	PO BOX 148
	FLAGLER BEACH FL 32136
Physical Address:	149 1ST ST, HOLLY HILL 32117
Property Use:	1000 - VACANT COMM
Tax District:	203-HOLLY HILL
2023 Final Millage Rate:	18.223
Neighborhood:	7230
Subdivision Name:	
Homestead Property:	No

Attachment: Exhibit B2 - KBL Property Investments, LLC (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

EXHIBIT C

LOCATION MAP



EXHIBIT D

AERIAL MAP



Attachment: Exhibit D - Aerial Map (2024-O-3079 : Mason Avenue Storage Facility Planned Development)

EXHIBIT E

FLU IS COMMERCIAL

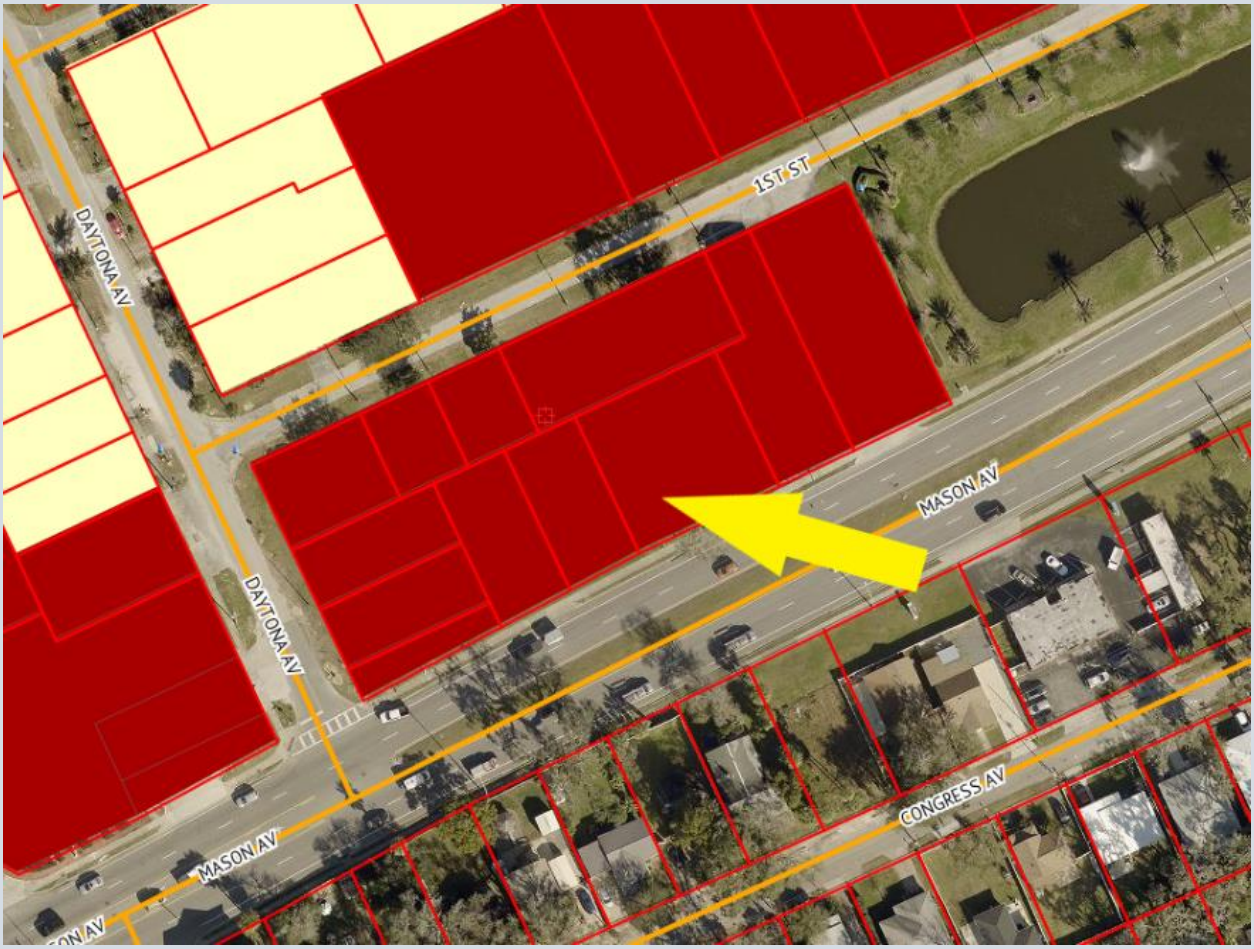
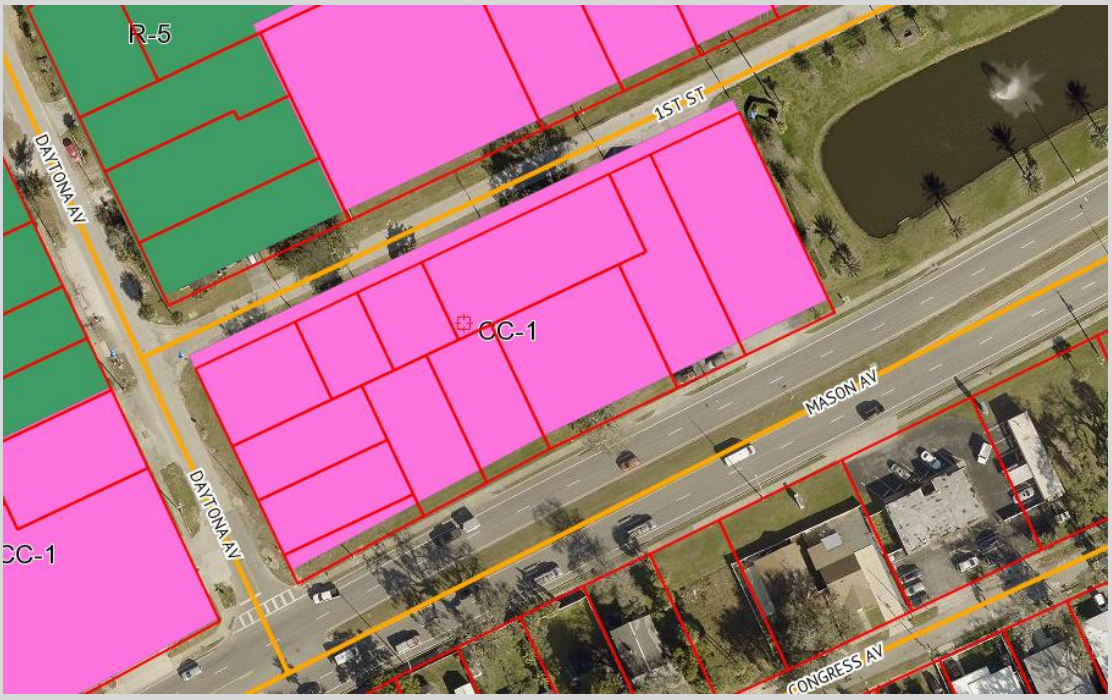
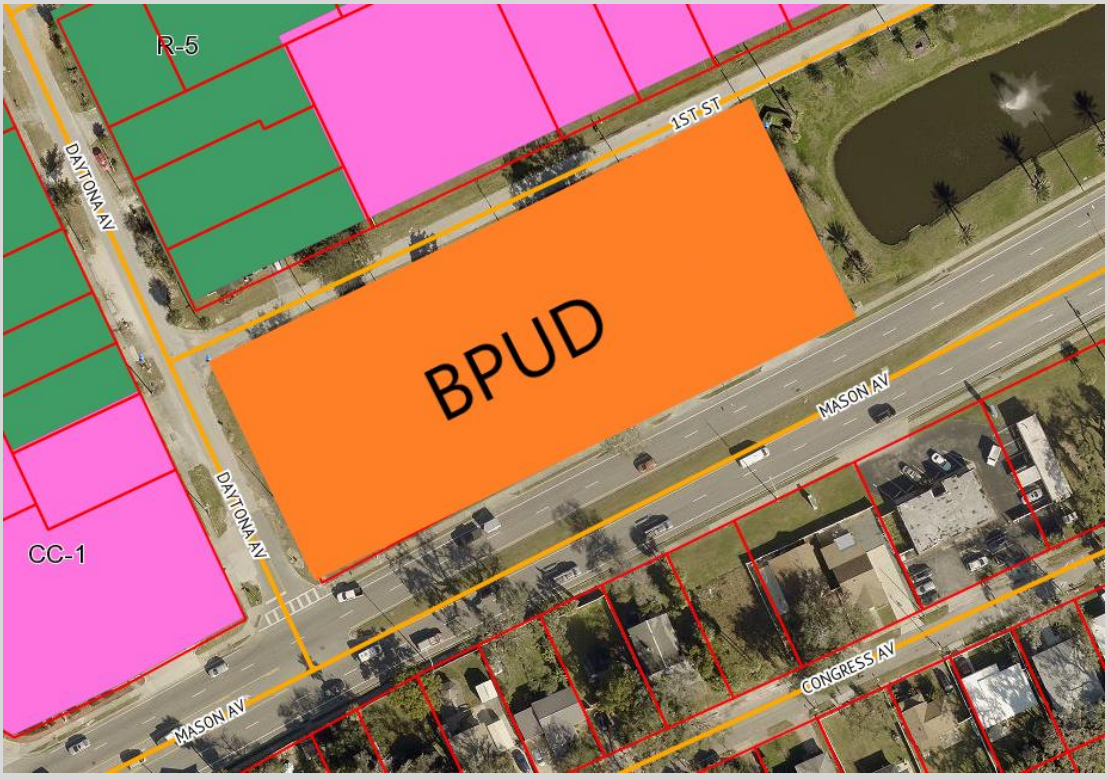


EXHIBIT F

CURRENT ZONING – CC-1



PROPOSED ZONING – BUSINESS PLANNED UNIT DEVELOPMENT





Not within a SFHA