OFFICE OF INSPECTOR GENERAL
PALM BEACH COUNTY

John A. Carey
Inspector General

Inspector General
Accredited

"Enhancing Public Trust in Government"

Audit Report

2024-A-0002

Town of Manalapan - IT Network Security Review

March 18, 2024

OFFICE OF INSPECTOR GENERAL
PALM BEACH COUNTY

AUDIT REPORT
2024-A-0002

DATE ISSUED: MARCH 18, 2024

John A. Carey
Inspector General

Inspector General
Accredited

"Enhancing Public Trust in Government"

TOWN OF MANALAPAN - IT NETWORK SECURITY REVIEW

SUMMARY

WHAT WE DID

We conducted an Information Technology (IT) Network Security review of the Town of Manalapan (Town).[1] This review was performed as part of the Office of Inspector General (OIG), Palm Beach County 2023 Audit Plan.

Our review focused on IT network security records and activities related to network components, such as devices, systems, and data, in place during fiscal year (FY) 2023 (October 1, 2022 to September 30, 2023).

WHAT WE FOUND

We found that the Town had processes in place designed to (a) prevent network security intrusions; (b) monitor and detect network security threats, breaches, and intrusions; and, (c) respond to network security threats, breaches, and intrusions.

However, the Town lacked sufficient written guidance for: (a) access control management; (b) data asset/component sanitization and disposal, and (c) organizational cybersecurity processes.

WHAT WE RECOMMEND

Our report contains three (3) findings and eight (8) recommendations. Implementation of the recommendations will assist the Town in strengthening internal controls over IT Network Security.

The Town concurred and accepted the recommendations.

We have included the Town's management response as Attachment 1.

[1] This was a standard, non-technical, compliance-type review where we verified the existence of basic IT network security practices and controls. Therefore, this review does not preclude the need for more comprehensive or in-depth assurance or advisory services, such as IT risk assessments, audits, and penetration testing.

BACKGROUND

The Town was incorporated in 1931 under Chapter 15684, Laws of Florida. The Town is unique in that two separate areas exist, contiguous only by water. That portion along A1A between Lantana Public Beach and South Lake Worth Inlet, more commonly known as Boynton Inlet, is the best-known area because of travel along the main north/south highway. Sharing Hypoluxo Island with the Town of Lantana, the area of Manalapan occupies about the southern one-third of the island. The Town's 2022 population was approximately 422.[2]

The current Town Charter was adopted on November 4, 2003, and it has been amended from time to time. The Town provides general municipal services such as police and fire protection. Additionally, the Town provides water to the residents of Manalapan and Hypoluxo from the municipal water plant located on U.S. Highway 1 in Hypoluxo.

The government of the Town is vested in the Town Commission, which is composed of seven (7) members elected to staggered two (2) year terms. No person can serve more than three (3) consecutive two (2) year terms in any elected office (Commissioner or Mayor) nor more than four (4) consecutive two (2) year terms in any combination of Commissioner and Mayor.

The Town Manager is the chief administrative officer. The Town Commission appoints the Town Manager for an indefinite term by a majority vote of all of the Commissioners. The Town Manager may be removed by a majority vote of all the Town Commissioners and, upon demand by the Town Manager, a public hearing shall be held prior to the vote.

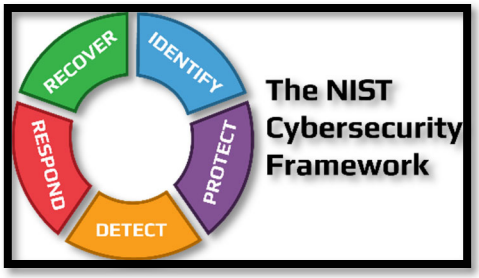
The OIG FY 2023 Annual Audit Plan included IT Network Security Reviews. The Town of Manalapan was selected for review because it operates a water utility, which increases the Town's IT Network Security risk. Additionally, the Town is small in terms of size and budget compared to many municipalities in Palm Beach County and operates a Police department; both factors further increase IT Network Security risk.

[2] http://edr.state.fl.us/Content/population-demographics/data/2022_Pop_Estimates.pdf

OIG IT NETWORK SECURITY REVIEW CHECKLIST

NIST Framework

The National Institute of Standards and Technology (NIST)[3] created a cybersecurity risk framework for use by critical infrastructure owners and operators. The NIST Framework Core consists of five interrelated functions—Identify, Protect, Detect, Respond, and Recover.



- **Identify** – Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.
- **Protect** – Develop and implement appropriate safeguards to ensure delivery of critical services.
- **Detect** – Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.
- **Respond** – Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.
- **Recover** – Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

NIST Security and Privacy Controls

The NIST Security and Privacy Controls publication[4] establishes controls for systems and organizations that process, store, or transmit information. The publication was designed to help organizations identify the controls necessary to manage security and privacy risk and is intended to be used by a diverse audience.

> 1.2 TARGET AUDIENCE
> This publication is intended to serve a diverse audience, including:
>
> - Individuals with system, information security, privacy, or risk management and oversight responsibilities, including authorizing

[3] As part of the U.S. Department of Commerce, NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems. The State of Florida Cybersecurity Standards, Rules 60GG-2.001 through 60GG-2.006, Florida Administrative Code, are modeled after the NIST Framework and the Federal Information Security Management Act of 2002. NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

Additionally, as of July 1, 2022, Section 282.3185, Florida Statutes, the "Local Government Cybersecurity Act," requires municipalities to adopt cybersecurity standards consistent with generally accepted best practices for cybersecurity, including the National Institute of Standards and Technology.

[4] NIST Special Publication 800-53, Revision 5, Security and Privacy Controls for Information Systems and Organizations.

officials, chief information officers, senior agency information security officers, and senior agency officials for privacy;

…

- Individuals with logistical or disposition-related responsibilities, including program managers, procurement officials, system integrators, and property managers;

…

- Individuals with security and privacy assessment and monitoring responsibilities, including auditors, Inspectors General, system evaluators, control assessors, independent verifiers and validators, and analysts;…

The NIST Security and Privacy Controls includes, but is not limited to the following control groups:

- Access Control
- Audit and Accountability
- Identification and Authentication
- Media Protection
- Awareness and Training
- Contingency Planning
- Incident Response
- Risk Assessment
- Personally Identifiable Information Processing and Transparency

CIS Critical Security Controls

The Center for Internet Security (CIS)[5] Critical Security Controls publication was developed to assist organizations with focusing their efforts on defending themselves against cybersecurity attacks. Critical Security Controls were advanced by combining the knowledge of subject matter experts in the public and private sectors. An organization can integrate Critical Security Controls commensurate with its IT maturity.

Implementation Guidance (IG) 1 controls

IG1 controls are suited for small to medium-sized organizations with limited IT and cybersecurity expertise dedicated to protecting IT assets and personnel. These controls focus on thwarting general, non-target attacks and are designed to work in conjunction with commercial off-the-shelf hardware and software. IG1 control groups include:

[5] The Center for Internet Security (CIS) is a community-driven 501(c)(3) nonprofit organization, formed in October 2000. Its mission is to make the connected world a safer place by developing, validating, and promoting timely best practice solutions that help people, businesses, and governments protect themselves against cyber threats. The organization is headquartered in East Greenbush, New York, with members including large corporations, government agencies, and academic institutions. https://www.cisecurity.org/about-us

- Inventory and Control of Enterprise Assets
- Inventory and Control of Software Assets
- Secure Configuration of Enterprise Assets and Software
- Data Protection
- Account Management
- Access Control Management
- Continuous Vulnerability Management
- Audit Log Management
- Email and Web Browser Protections
- Malware Defenses
- Data Recovery
- Network Infrastructure Management
- Security Awareness and Skills Training
- Service Provider Management
- Incident Response Management

IG2 controls

IG2 controls are suited for enterprises employing individuals who are responsible for managing and protecting IT infrastructure. Often these organizations have regulatory burdens related to processing and storing sensitive customer information. These controls help security teams manage operational complexity. In addition to the IG1 control groups, IG2 control groups include:

- Network Monitoring and Defense
- Application Software Security
- Penetration Testing

IG3 controls

IG3 controls are suited for enterprises that employ security experts who specialize in cybersecurity risk management, penetration testing and application security. IG3 controls strengthen the IG1 and IG2 control groups in an effort to mitigate targeted attacks from sophisticated adversaries.

IT Network Security Review Checklist

We developed an IT Network Security Review checklist of cybersecurity activities and controls centered on the NIST Framework Core, which is a set of cybersecurity activities, desired outcomes, and references that are common across critical infrastructure sectors. The IT Network Security Review checklist focuses on activities and controls recommended in the NIST Special Publication 800-53 (Revision 5) Security and Privacy Controls for Information Systems and Organizations (Security and Privacy Controls), the use of which is mandatory for federal information systems; and, the CIS Critical Security Controls (Version 8) IG1,[6] which are considered "essential cyber hygiene" that can be implemented with limited cybersecurity expertise aimed to thwart general, non-targeted attacks.

We developed our IT Network Security Review checklist to include activities and controls related to:

1. Physical Devices (Hardware)
2. Account Management (User and Administrative)
3. Organizational Cybersecurity Policy

[6] https://www.cisecurity.org/controls

4. Access Control Management
5. Disposition of Data
6. Malware Defenses
7. Email and Web Browser Protections
8. Network Security Awareness Program and Training
9. Incident Management Response Plan
10. Contingency/Recovery Planning

OBJECTIVES, SCOPE, AND METHODOLOGY

The overall objectives of the review were to determine whether the Town had processes in place designed to:

1) Prevent network security intrusions;
2) Monitor and detect network security threats, breaches, and intrusions; and,
3) Respond to and eliminate network security threats, breaches, and intrusions.

The scope of the review was limited to IT network security records and activities related to significant IT network components, such as devices, systems, and data, in place during fiscal year (FY) 2023.

The review methodology included but was not limited to:

- Reviewing ordinances, policies, procedures, and related requirements;
- Conducting a review of IT Network Security processes and controls based on the NIST Framework for Improving Critical Infrastructure Cybersecurity and, the CIS Critical Security Controls;
- Interviewing appropriate personnel; and,
- Reviewing records, logs, and reports.

This review was conducted in accordance with the Principals and Standards for Offices of Inspector General. Those standards require that we plan and perform the review to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our review objectives. We believe that the evidence we obtained provides a reasonable basis for our findings and conclusions based on our review objectives.

FINDINGS AND RECOMMENDATIONS

Finding (1): The Town lacked sufficient written guidance for access control management.

Section 218.33, Florida Statutes (2019), states,

> (3) Each local government entity shall establish and maintain internal controls designed to:
>
> (a) Prevent and detect fraud, waste, and abuse as defined in s. 11.45(1).

(b) Promote and encourage compliance with applicable laws, rules, contracts, grant agreements, and best practices.
(c) Support economical and efficient operations.
(d) Ensure reliability of financial records and reports.
(e) Safeguard assets.[7]

The NIST Framework describes identity management and access control as ensuring access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices and is managed consistent with the associated risk of unauthorized access to authorized devices and transactions.

The NIST Security and Privacy Controls for access control management processes includes having account management, access enforcement, separation of duties, least privilege,[8] access control for mobile devices, and identification and authentication processes and procedures. The CIS Critical Security Controls IG1 includes processes and tools to assign and manage authorization credentials as well as create, assign, manage, and revoke access credentials, and privileges for user, administrative, and service accounts.

Access control management controls include but are not limited to:

- Establishing an account management process for assigning and managing user account authorizations;
- Establishing an access granting process upon new hire, rights grant, or a role change;
- Establishing an access revoking process through disabling accounts immediately upon termination, rights revocation, or role change;
- Identifying, and dividing, business and support functions between different individuals, or roles, to reduce risk associated with authorized privileges abuse;
- Employing the principal of least privilege, allowing only authorized access for users that are necessary to accomplish assigned organizational tasks; and,
- Establishing unique identification and authentication requirements (usernames, passwords, biometrics) for user accounts accessing the network.

We found that the Town has processes with controls to assist with granting and revoking user access to the network, maintaining role-based control and documenting access rights for each role to carry out assigned duties, employing the principle of least privilege, and maintaining secure configuration of enterprise assets and software to include requiring unique user IDs and passwords, automatic logouts after periods of inactivity, screensavers, and multifactor authentication. However, the Town did not have an implemented IT Policy or procedures documenting the processes and controls prior to commencement of our review.

[7] As of July 1, 2022, Section 282.3185, Florida Statutes, requires municipalities to adopt cybersecurity standards consistent with generally accepted best practices for cybersecurity, including National Institute of Standards and Technology Cybersecurity Framework based on their population. The Town's effective date is January 1, 2025.

[8] Only the minimum necessary rights should be assigned to a subject that requests access to a resource and should be in effect for the shortest duration necessary.

A lack of written policies and procedures for access control management increases the risk of data breaches and unauthorized access and modification of enterprise systems and data because users have access to critical or sensitive data and systems that is not necessary to perform their roles and responsibilities within the organization.

Corrective Action:

We reviewed the Town's IT Policy implemented during our review, which was effective as of August 28, 2023, and found it includes guidance for assigning and managing user account authorizations; granting access upon new hire; limiting access based on roles/responsibilities; when necessary, revoking access; and, maintaining secure configuration of enterprise assets and software to include requiring unique user IDs, passwords, and screensavers.

Recommendations:

(1) The Town develop and implement a written Access Control Management policy and procedure that provides guidance including:

- **a. Establishing an account management process for assigning and managing user account authorizations;**
- **b. Establishing an access granting process upon new hire, rights grant or a role change;**
- **c. Establishing an access revoking process through disabling accounts immediately upon termination, rights revocation, or role change;**
- **d. Identifying and dividing business and support functions between different individuals or roles to reduce risk associated with authorized privileges abuse;**
- **e. Employing the principal of least privilege, allowing only authorized access for users that are necessary to accomplish assigned organizational tasks; and,**
- **f. Establishing unique identification and authentication requirements (usernames, passwords, biometrics, etc.) for user accounts accessing the network.**

(2) The Town ensure staff are aware of their roles and responsibilities related to access control management.

Management Response:

Management accepts the findings and recommendations. The Town has since implemented new language in our IT policy (as noted in the draft audit report you provided) to address this finding and it can be found specifically in section V. Access Control and Authentication Mechanisms, subsections A. Access Philosophy, B. Default Facilities, C. Departures from The Town of Manalapan, D. Unique User Ids, And E Password.

Finding (2): The Town lacked sufficient written guidance for data and asset/component sanitization and disposal.

Section 218.33, Florida Statutes (2019), states,

> (3) Each local government entity shall establish and maintain internal controls designed to:
> (a) Prevent and detect fraud, waste, and abuse as defined in s. 11.45(1).
> (b) Promote and encourage compliance with applicable laws, rules, contracts, grant agreements, and best practices.
> (c) Support economical and efficient operations.
> (d) Ensure reliability of financial records and reports.
> (e) Safeguard assets.

The NIST Framework describes information protection processes and procedures as security policies, processes, and procedures that are used to manage the protection of information systems and assets. The NIST Security and Privacy Controls for information protection processes and procedures include having media and component sanitization and disposal processes and procedures. Additionally, the CIS Critical Security Controls IG1 includes data protection controls to securely dispose of data stored on the network, whether it is stored remotely or on enterprise assets and devices.

Data and asset/component sanitization and disposal controls include but are not limited to:

- Establish and maintain a data management process that addresses data retention limits and disposal requirements and ensures the disposal process and method is commensurate with the data sensitivity;
- Reviewing and approving assets to be sanitized to ensure compliance with record retention requirements;
- Tracking and documenting actions including listing personnel who reviewed and approved sanitization and disposal actions, types of assets sanitized, files stored on the asset, sanitization methods used, date and time of the sanitization actions, personnel who performed the sanitation, verification actions taken and personnel who performed the verification, and the disposal actions taken;
- Disposing of data, documentation, tools, or system components as outlined in the data management process;
- Verifying that the sanitization of the asset was effective prior to disposal; and,
- Testing of sanitation equipment and procedures.

We found that the Town had processes with controls to assist with data and asset/component sanitization and disposal; however, there were no written policies or procedures documenting the processes and controls in place prior to the commencement of our review. We reviewed the Town's IT Policy implemented during our review, which was effective as of August 28, 2023; however, it did not include sufficient controls and written guidance related to the Town's data and asset/component sanitization and disposal process.

A lack of written policies and procedures for data and asset/component sanitization and disposal increases the risk associated with loss of control over protected or sensitive data.

Recommendations:

(3) The Town develop and implement a written Data Sanitization and Asset/Inventory Disposal policies and procedures that provide guidance regarding:

a. Establishing and maintaining a data management process that addresses data retention limits and disposal requirements and ensures the disposal process and method are commensurate with the data sensitivity;

b. Reviewing and approving assets to be sanitized to ensure compliance with record retention requirements;

c. Tracking and documenting actions including listing personnel who reviewed and approved sanitization and disposal actions, types of assets sanitized, files stored on the asset, sanitization methods used, date and time of the sanitization actions, personnel who performed the sanitation, verification actions taken and personnel who performed the verification, and the disposal actions taken;

d. Disposing of data, documentation, tools, or system components as outlined in the data management process;

e. Verifying that the sanitization of the asset was effective prior to disposal; and,

f. Testing of sanitation equipment and procedures.

(4) The Town ensure staff are aware of their roles and responsibilities related to data and asset/component sanitization and disposal.

Management Response:

Management accepts the findings and recommendations. The Town has since implemented new language in our IT policy (as noted in the draft audit report you provided) to address this finding and it can be found specifically in section X. Data and Asset/Component Sanitization, Destruction, and Disposal, subsections A. Purpose, B. Scope C. Data Sanitization D. Asset/Component Disposal, E. Documentation and Verification F. Responsibilities G. Compliance.

Finding (3): The Town lacked sufficient written guidance for the organizational cybersecurity process.

Section 218.33, Florida Statutes (2019), states,

> (3) Each local government entity shall establish and maintain internal controls designed to:
> (a) Prevent and detect fraud, waste, and abuse as defined in s. 11.45(1).
> (b) Promote and encourage compliance with applicable laws, rules, contracts, grant agreements, and best practices.
> (c) Support economical and efficient operations.
> (d) Ensure reliability of financial records and reports.
> (e) Safeguard assets.

The NIST Framework describes governance as the policies, procedures and processes implemented by an organization to manage and monitor regulatory, legal, environmental, and operational requirements that inform management of cybersecurity risk. The NIST Security and Privacy Controls for Governance of Cybersecurity include having a documented Incident Response Plan and a documented Contingency/Recovery Plan. Additionally, the CIS Critical Security Controls IG1 includes establishing an Incident Response Management program to develop and maintain incident response capability (e.g. policies, plans, procedures, defined roles, training, and communications) to prepare, detect, and quickly respond to an attack, as well as a Data Recovery process to restore in-scope enterprise assets to a pre-incident and trusted state.

Incident Response Plan controls include:

- Designating one key person, and at least one backup, who will manage the incident handling process;
- Establishing and maintaining contact information for parties that need to be informed of security incidents;
- Establishing and maintaining a process for staff to report security incidents;
- Testing to determine the effectiveness of the plan to identify weaknesses or deficiencies; and,
- Tracking and documenting security incidents.

Contingency/Recovery Plan controls include:

- Identifying essential mission and business functions and associated contingency requirements;
- Identifying recovery objectives and restoration priorities;
- Addressing contingency roles, responsibilities, and assigned individuals with contact information;
- Addressing maintaining essential mission and business functions despite a system disruption, comprise, or failure;
- Addressing eventual, full system restoration without deterioration of the controls originally planned;

- Testing to determine the effectiveness, and readiness, of the plan to identify potential weaknesses; and,
- Safeguarding and testing of backup information to ensure it can be reliably retrieved and restored for essential mission and business functions.

We found that the Town had processes with controls to assist with continuity of operations should it be exposed to a cybersecurity incident; however, it did not have written IT policies and procedures in place prior to our review.

Corrective Action

We reviewed the Town's IT Policy implemented during our review and found it designated responsibilities for and established processes to manage and monitor cybersecurity risks, including an Incident Response Plan:

- Designating one key person, and at least one backup, who will manage the incident handling process;
- Establishing and maintaining contact information for parties that need to be informed of security incidents;
- Establishing and maintaining a process for staff to report security incidents;
- Testing to determine the effectiveness of the plan to identify weaknesses or deficiencies; and,
- Tracking and documenting security incidents.

Additionally, the implemented IT Policy provides Contingency/Recovery plan guidance on backing up critical information and critical software maintained on Town server systems. However, it did not include a sufficient Contingency/Recovery plan because the policy did not provide recovery objectives, restoration priorities, and metrics; address contingency roles and responsibilities; assign individuals with contact information; address maintaining essential mission and business functions despite a system disruption, compromise, or failure (i.e. procedures and documentation while systems are not functioning); address eventual, full system restoration without the deterioration of the controls originally planned and implemented; and, address testing of the plan and backup information to determine effectiveness and readiness, and identify potential weaknesses.

Moreover, the Town's IT Policy refers to a Disaster Recovery Plan whereby "the Town Manager's Office will assist in the preparation, periodical update, and testing of a disaster recovery plan that will permit all critical computer and communication systems to be available in the event of a major loss such as may be caused by the event of nature or a catastrophe." However, the Town confirmed that there is no Disaster Recovery Plan separate from what is identified in the IT Policy.

A lack of sufficient written policies and procedures for the organizational cybersecurity process to include incident response and contingency/recovery processes increases the risk associated with identifying and responding to network threats and continuity of operations during and after a cybersecurity incident.

Recommendations:

(5) The Town implement an IT policy that ensures cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners, and include governance and risk management processes addressing cybersecurity risks.

(6) The Town develop and implement written Incident Response Plan policies and procedures to ensure continuity of operations that provide guidance, at a minimum, including:

- **a. Designating one key person, and at least one backup, who will manage the incident handling process;**
- **b. Establishing and maintaining contact information for parties that need to be informed of security incidents;**
- **c. Establishing and maintaining a process for staff to report security incidents;**
- **d. Testing to determine the effectiveness of the plan to identify weaknesses or deficiencies; and,**
- **e. Tracking and documenting security incidents.**

(7) The Town develop and implement written Contingency/Recovery Plan policies and procedures to ensure continuance of mission and business functions that provide guidance, at a minimum, including:

- **a. Identifying essential mission and business functions and associated contingency requirements;**
- **b. Identifying recovery objectives and restoration priorities;**
- **c. Addressing contingency roles, responsibilities, and assigned individuals with contact information;**
- **d. Addressing maintaining essential mission and business functions despite a system disruption, comprise, or failure;**
- **e. Addressing eventual, full system restoration without deterioration of the controls originally planned;**
- **f. Testing to determine the effectiveness, and readiness, of the plan to identify potential weaknesses; and,**
- **g. Safeguarding and testing of backup information to ensure it can be reliably retrieved and restored for essential mission and business functions.**

(8) The Town ensure staff are aware of their roles and responsibilities in responding to and recovering from a network security incident, including maintaining business functions during a system disruption or failure.

Management Response:

Management accepts the findings and recommendations. The Town has since implemented new language in our IT policy (as noted in the draft audit report you provided) to address this finding and it can be found throughout the entirety of the Town's IT policy and more specifically in sections III. Information Security Policies,

IV. Information Security, V. Access Control and Authentication Mechanisms, VI. Operations Management, VII. Security Incident Response Policy, VIII. Detection and Analysis, and section IX. Containment, Eradication, and Recovery.

ACKNOWLEDGEMENT

The Inspector General's audit staff would like to extend our appreciation to the Town of Manalapan's staff for their assistance and support in the completion of this review.

This report is available on the OIG website at: https://www.pbcgov.com/OIG. Please address inquiries regarding this report to the Director of Audit by email at inspector@pbc.gov or by telephone at (561) 233-2350.

ATTACHMENT

Attachment 1 – Town of Manalapan's Management Response

ATTACHMENT 1 – TOWN OF MANALAPAN'S MANAGEMENT RESPONSE

TOWN OF MANALAPAN
600 South Ocean Boulevard, Manalapan, Florida 33462-3398
Telephone (561) 585-9477 Fax (561) 585-9498
Email: townhall@manalapan.org www.manalapan.org

3/15/2024
Hillary Bojan, Director of Audit
Palm Beach County Office of Inspector General
PO Box 16568
West Palm Beach, Florida 33416

Re: Draft Audit Report – Manalapan IT Network Security Review

Dear Ms. Bojan:

On behalf of the Town of Manalapan, we appreciate the opportunity to respond to the draft audit report referenced above. In accordance with the request, we will address the findings and recommendations outlined in the report and propose the following actions. Each action is referenced in our response in the attached document titled "Town of Manalapan IT Policy - Final 2024".

Finding 1: The Town lacked sufficient written guidance for access control management.

Management accepts the findings and recommendations. The Town has since implemented new language in our IT policy (as noted in the draft audit report you provided) to address this finding and it can be found specifically in section V. Access Control and Authentication Mechanisms, subsections A. Access Philosophy, B. Default Facilities, C. Departures from The Town of Manalapan, D. Unique User Ids, And E Password.

Finding 2: The Town lacked sufficient written guidance for data and asset/component sanitization and disposal. Management accepts the findings and recommendations. The Town has since implemented new language in our IT policy (as noted in the draft audit report you provided) to address this finding and it can be found specifically in section X. Data and Asset/Component Sanitization, Destruction, and Disposal, subsections A. Purpose, B. Scope C. Data Sanitization D. Asset/Component Disposal, E. Documentation and Verification F. Responsibilities G. Compliance.

Finding 3: The Town lacked sufficient written guidance for the organizational cybersecurity process. Management accepts the findings and recommendations. The Town has since implemented new language in our IT policy (as noted in the draft audit report you provided) to address this finding and it can be found throughout the entirety of the Town's IT policy and more specifically in sections III. Information Security Policies, IV. Information Security, V. Access Control and Authentication Mechanisms, VI.

TOWN OF MANALAPAN
600 South Ocean Boulevard, Manalapan, Florida 33462-3398
Telephone (561) 585-9477 Fax (561) 585-9498
Email: townhall@manalapan.org www.manalapan.org

Operations Management, VII. Security Incident Response Policy, VIII. Detection and Analysis, and section IX. Containment, Eradication, and Recovery.

In conclusion, the Town extends its sincere gratitude to the Office of the Inspector General for their exceptional public service in conducting a comprehensive review of our IT operations. We appreciate the time and effort taken to provide detailed recommendations that significantly enhance the Town's protection against various threats. We believe we have implemented the necessary changes based on your office's recommendations and have distributed the updated policy to all town staff to ensure their awareness and compliance.

Sincerely,

Eric Marmer
Assistant Town Manager