

**The Maryland-National Capital Park and Planning Commission  
Office of the Inspector General**

**Cybersecurity Incident Response  
Report Number: CW-003-2026**

**October 16, 2025**

**Distribution:**

Audit Committee

Mitra Pedoeem

Erin White

Benjamin Williams

Maryland-National Capital Park and Planning Commission

Todd Allen

Darryl Barnes

Joe Bistany

Debra Borden

James Cannistra

Mazen Chilet

Gavin Cohen

Miti Figueredo

Artie Harris

Tracey Harvin

Vince Hu

Lakisha Hull

Ike Onyegbado

William Rhodes

Jason Sartori

William Spencer

Darius Stanton

Office of the Inspector General

Renee Kenney

Modupe Ogunduyile

Aaron Smith

Irith Dror

**Cybersecurity Incident Response**  
Table of Contents

**I. EXECUTIVE SUMMARY**

A. Overall perspective.....	1
B. Audit Objective, Scope, and Methodology.....	2
C. Major Audit Concerns.....	3
D. Overall Conclusions.....	4

**II. DETAILED COMMENTARY AND RECOMMENDATIONS**

1. Update and Implement the Commission-Wide Cybersecurity Incident Response Policy to Increase Coordination of Incident Response.....	5
2. Conduct Tabletop Exercises Annually.....	8

**III. EXHIBITS**

A. Incident Response and Management Policy Overview Section.....	10
B. M-NCPPC Cybersecurity Incident Response Plan Summary.....	11

## I. EXECUTIVE SUMMARY

### A. Overall Perspective

Cyber-attacks pose significant threats to organizations, potentially impacting them in various ways that could lead to financial loss, data breaches and operational disruption. To reduce the harm associated with cybersecurity incidents, organizations' Information Technology (IT) departments commonly administer a cybersecurity incident response policy that provides the guidelines for incident response capabilities, and an incident response plan that details how to monitor, identify and respond to cybersecurity incidents.

The Maryland National Park and Planning Commission (Commission or M-NCPPC) has, at the corporate level, a Chief Information Officer (CIO) and an Information Security Officer (ISO). In addition, at the Department level, there are four IT Division Chiefs (referred to as Chief Technology Officers – CTOs) who are responsible for providing IT support to their respective areas. See **Table 1** for Commission IT Personnel.

**Table 1. Commission IT Management Personnel**

Name	Title	Department
Mazen Chilet	Chief Information Officer (CIO)	Office of the CIO
Ike Onyegbado	Information Security Officer (ISO)	Office of the CIO
Joe Bistany	CTO, Enterprise Information Technology	Office of the CIO
James Cannistra	CTO, Information Management Division	Prince George's County Planning
Vince Hu	CTO, Information Technology and Innovation	Montgomery Parks and Montgomery Planning
William Rhodes	CTO, Information Technology Services	Prince George's County Parks and Recreation (DPR)

In 2020, the Office of the CIO (OCIO) established both a Commission wide Incident Response and Management Policy and an Incident Response Plan. See **Exhibits A and B**. In addition, each department has their own cybersecurity incident response plan and procedures in place.

## **B. Audit Objective, Scope, and Methodology**

### Audit Objective

The objective of this audit was to evaluate the internal controls for cybersecurity incident response processes. Properly implemented internal controls reduce financial, reputational, and operational risks within the organization.

### Scope

The scope for the audit for Cybersecurity Incident Response included, but was not limited to, the following audit procedures:

- Reviewing cybersecurity incident response policies and plans
- Evaluating the effectiveness of incident response plans
- Analyzing Commission-wide incident tracking, reporting and review protocols;
- Interviewing IT personnel involved with cybersecurity management
- Reviewing the 2024 Securance report to determine if the recommendations were implemented<sup>1</sup>

In addition, the audit scope was designed to identify possible fraud, waste, or abuse within the processes being audited

The period covered in this review was January 1, 2024 through June 30, 2025.<sup>2</sup>

### Methodology

During the audit, the auditor-in-charge conducted interviews of management and staff, and reviewed relevant standard operating procedures, Commission policies, and organizational charts. For our analysis, we obtained and reviewed incident response reports and data obtained from cybersecurity applications.

This audit was conducted in accordance with *Generally Accepted Government Auditing Standards*. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

---

<sup>1</sup> In March 2024, Securance Consulting reviewed the Commission's incident response plan and vulnerability management process.

<sup>2</sup> Audit Scope extended from April 01, 2025 to June 30, 2025

**C. Major Audit Concerns**

The results of our evaluation and testing procedures indicated no major audit concerns.

## D. Overall Conclusions


The results of our evaluation and testing procedures indicate no major weaknesses in the design or operation of internal controls for Cybersecurity Incident Response. On an overall basis, we consider the controls to be satisfactory.

We believe all weaknesses identified and communicated are correctable and that management's responses to all recommendations satisfactorily address the concerns. It is the responsibility of management to weigh the possible additional costs of implementing our recommendations in terms of benefits to be derived and the relative risks involved.

We wish to express our appreciation to management and staff for the cooperation and courtesies extended during the course of our review.

*Aaron Smith*

Aaron Smith, CIGA  
Auditor

  
Irith Dror (Oct 15, 2025 14:40:23 EDT)

Irith Dror  
Senior IT Auditor

*Modupe Ogunduyile*

Modupe Ogunduyile, CIG  
Deputy Inspector General

*Renee Kenney*

Renee M. Kenney, CIG, CPA, CIA, CISA  
Inspector General

October 16, 2025

### Conclusion Definitions

<b>Satisfactory</b>	No major weaknesses were identified in the design or operation of internal control procedures.
<b>Deficiency</b>	A deficiency in the design or operation of an internal control procedure(s) that could adversely affect an operating unit's ability to safeguard assets, comply with laws and regulations, and ensure transactions are properly executed and recorded on a timely basis.
<b>Significant Deficiency</b>	A deficiency in the design or operation of an internal control procedure(s) which adversely affects an operating unit's ability to safeguard assets, comply with laws and regulations, and ensure transactions are properly executed and reported. This deficiency is less severe than a material weakness, yet important enough to merit attention by management.
<b>Material Weakness</b>	A deficiency in the design or operation of an internal control procedure(s) which may result in a material misstatement of the Commission's financial statements or material impact to the Commission.

## II. DETAILED COMMENTARY AND RECOMMENDATIONS

### 1. Update and Implement the Commission-Wide Cybersecurity Incident Response Policy to Increase Coordination of Incident Response.

**Issue:** The OIG reviewed the cybersecurity incident response plan and procedures from each department and determined that the tracking and resolution of cybersecurity incidents was sufficient. However, the Office of the Chief Information Officer's (OCIO) policy, issued in June 2020, does not provide adequate guidance for departmental level cybersecurity incident response plans and procedures:

- There are no criteria established in the OCIO's policy to prioritize and escalate incidents. The Office of the Inspector General (OIG) reviewed a sample of incident records from each department and compared them with the contents of the Commission-wide Incident Report Portal. Between January 1, and April 30, 2025, 414 incidents classified as high/severe throughout the Commission were tracked by each department. No incidents were logged into the Commission-wide portal during this period<sup>3</sup>.
- The OCIO's policy does not contain definitions of events or cybersecurity incidents, such as what qualifies as a cybersecurity incident.
- The OCIO's policy does not identify incident response team members and does not contain details of specific roles in escalation procedures.
- The OCIO's policy does not directly establish whether each department should have their own cybersecurity incident response plans in place. The OIG determined that the Enterprise IT Department's cybersecurity incident response plan has not been updated since 2010. Additionally, Montgomery Parks and Montgomery Planning Departments do not have a cybersecurity incident response plan formally documented.

**Criteria:** NIST SP 800-61r3 states most incident response policies include the same key elements:

- Statement of management commitment
- Purpose and objectives of the policy
- Scope of the policy
- Definition of events, cybersecurity incidents, investigations and related terms

---

<sup>3</sup> The Office of the CIO's policy requires all incidents to be logged using the established Commission-wide incident logging process/system. See **Exhibit A-**

Cybersecurity Incident Response  
Report No. CW-003-2026

- Roles, responsibilities, and authorities, such as which roles have the authority to confiscate, disconnect, or shut down technology assets
- Guidelines for prioritizing incidents, estimating their severity, initiating recovery processes, maintaining or restoring operations and other key actions
- Performance measures

Processes and procedures should be based on the incident response policy and plan. Documented procedures should explain how technical process and other operating procedures should be performed.

**Cause:** The OCIO did not prioritize updating the Commission-wide Cybersecurity Incident Response policy to ensure consistency in the administration of cybersecurity incident response plans within each department.

**Risk:** The absence of an updated Commission-wide Cybersecurity Incident Response Policy impacts the Commission's ability to execute a coordinated response to cybersecurity incidents, including post incident analysis. Failure to update and implement this policy at the Commission-wide level increases the likelihood of financial loss, data breaches and operational disruption.

**Recommendation:** The OCIO should update the Commission-wide Cybersecurity Incident Response policy and it should be used as a guideline for establishing each department's incident response plan. The policy should include the following:

- Implement standard criteria to identify critical/high-level incidents and require the departments to log those incidents into the Commission-wide Incident Report Portal
- Identify the positions, roles and responsibilities of incident response team members from each department
- Require departments to document department level response plans, review them annually and update them as necessary
- Provide universal definitions of cybersecurity incidents and events

Furthermore, the Commission wide incident response policy should be reviewed annually and updated when necessary.

**Issue Risk:** Medium

**Management Response:** We acknowledge the findings and recommendations regarding the Commission-wide Cybersecurity Incident Response Policy. To address the deficiencies:

Cybersecurity Incident Response  
Report No. CW-003-2026

- We will revise the policy to include standardized definitions of cybersecurity events and incidents, aligned with NIST SP 800-61r3.
- We will define the roles and responsibilities of incident response team members, including escalation procedures, within the policy or its appendix.
- We will mandate that each department develop, maintain, and annually review a formal incident response plan. Compliance will be monitored through periodic audits.
- We will implement criteria for prioritizing and escalating incidents and require all high/severe incidents to be logged in the Commission-wide Incident Report Portal.
- We will establish an annual review cycle for the policy to ensure it remains current and effective.

These updates will be completed by September 4, 2026, and will be communicated to all departments with training and support to ensure consistent implementation.

**Expected Completion Date:** September 2026

**Follow-Up Date:** November 2026

## **2. Conduct Tabletop Exercises Annually**

**Issue:** Tabletop exercises help validate the content of cybersecurity incident response plans, provide a platform for training personnel to handle adverse events, and assist the organization's capacity to prepare for, respond to, and recover from a potential disaster. OIG determined that the incident response plans and procedures from Enterprise IT Department, Montgomery Parks and Montgomery Planning Department, and DPR have not been tested via a tabletop exercise.

**Criteria:** Per NIST Special Publication (SP) 800-84 tabletop exercises are discussion-based events where personnel with roles and responsibilities in a particular IT plan meet in a classroom setting or in breakout groups to discuss their roles during an emergency and their responses to a particular emergency situation. Tabletop exercises are cost-effective tools to validate the content of IT plans, such as incident response plans, to ensure the plan content is viable and implementable in an emergency situation.

**Cause:** Tabletop exercises were not conducted due to staffing and budgeting constraints.

**Risk:** Without conducting tabletop exercises, the Commission departments may not be ready to respond to cyberattacks, which may lead to the potential of financial loss, data breaches and operational disruption.

**Recommendation:** OIG recommends that each department perform a tabletop exercise of their respective incident response plan at least once annually.

**Issue Risk:** Medium

**Management Response:** We appreciate the Office of the Inspector General's review and recommendation emphasizing the importance of annual tabletop exercises to validate and enhance our cybersecurity incident response capabilities.

Management concurs with the recommendation. Tabletop exercises serve as a critical mechanism for assessing the effectiveness of incident response plans, training personnel, and reinforcing organizational readiness against evolving cyber threats. While staffing and budget constraints have previously limited our ability to conduct these exercises consistently across all departments, we recognize the need to close this gap.

To that end, tabletop exercises will be incorporated as an optional component of the annual Cybersecurity-as-a-Service (CSaaS) scope of work, allowing service providers to include them in their proposals. As part of a phased implementation strategy, we may leverage vendor-led facilitation during the initial one to three

Cybersecurity Incident Response  
Report No. CW-003-2026

years to establish a repeatable process and build internal capacity. Following this period, we intend to transition to in-house delivery informed by lessons learned and best practices.

This approach not only strengthens institutional capability but also promotes deeper team engagement through early collaboration with experienced vendors.

**Expected Completion Date:** August 2026

**Follow up Date:** November 2026

### III. Exhibits

#### **Exhibit A: Incident Response and Management Policy Overview Section**

1. The M-NCPPC OCIO shall oversee the group responsible for developing and implementing an incident response plan for all information system and data assets housing or accessing Commission controlled information. The core incident response team will be reflective and composed of (2) security team members from the M-NCPPC department IT units. The Information Security Officer (ISO) will lead the team in developing and implementing a robust incident response plan.
2. The M-NCPPC incident response policy requires all incidents to be logged using the established incident logging process/system. The incident logging process should be as automated as possible. A copy of the current M-NCPPC Security Incident Log Form can be found in Appendix B.
3. The ISO should be notified of all computer and network security incidents that may affect the confidentiality, availability and/or integrity of the computer equipment or information at M-NCPPC.
4. The M-NCPPC incident response plan will be tested on a quarterly basis to ensure it is up to date and in accordance with the current state of information systems and assets. Accepted forms of testing, including tabletop exercises or simulated tests, will be conducted based on the discretion of the ISO and the availability of required resources. M-NCPPC department IT units will report their testing results to the CIO and ISO.
5. Departmental IT Groups may use their own incident response procedures to supplement this incident response plan under the direction of the ISO
6. If the incident involves law enforcement or has legal ramifications, it is important to preserve the scene, document the situation, and not to destroy evidence that may reside within the system. There are forensic processes that must be adhered to and it is highly recommended that the ISO be involved, and a trained computer forensics expert be used or may require outside experts to handle.
7. The ISO will notify the CTOs and the CIO for incidents that involve protected information.

### **Exhibit B: M-NCPPC Cybersecurity Incident Response Plan Summary**

While cybersecurity related incidents may not be all preventable, proper planning and execution of an incident response plan makes a big difference relative to the occurrence, impact, efficient and timely remediation of an incident.

The M-NCPPC incident response plan builds on best practices as well as NIST SP 800-61 industry standard to define the necessary steps required to:

- Recognize and respond to an incident
- Quickly assess, classify and efficiently contain the situation

In addition, the plan details the steps to communicate with the appropriate business units, Information technology groups as well as other necessary entities relative to the mitigation of a cyber security incident.

Furthermore, the plan outlines the mechanism for activating relevant groups-like the Help Desk, The Microsoft Infrastructure Group as well as the M-NCPPC Security Team as and at when required to efficiently resolve an incident and return the impacted system and or IT Operations back to business as usual.