OFFICE *of the*
INSPECTOR GENERAL
U.S. GOVERNMENT PUBLISHING OFFICE

AUDIT REPORT

Cybersecurity Incident Response Maturity Assessment

Report Number OIG-26-06

March 30, 2026

Questions, Copies, Suggestions

The Audit Division, Office of the Inspector General, prepared this report. If you have questions about the report or would like additional copies, contact the Office of the Inspector General.

To suggest ideas for or request future audits of Government Publishing Office issues, contact the Office of the Inspector General at:

Hotline: 866-4-GPO-OIG (866-447-6644)

Fax: 202-512-1352

Email: gpoighotline@gpo.gov

Mail: Office of the Inspector General
Government Publishing Office
732 North Capitol St. NW
Washington, DC 20401

In accordance with the GPO Inspector General Act of 1988, the Inspector General Act of 1978, as amended, and GPO Office of Inspector General (OIG) policy, the GPO IG attempts to protect the confidentiality of a person who makes an allegation or provides information regarding wrongdoing unless the Inspector General determines such disclosure is unavoidable during the course of the investigation or disclosure is otherwise required by law.

Date:
March 30, 2026

To:
Director, U.S. Government Publishing Office

From:
Inspector General

Subject:
Audit Report: Cybersecurity Incident Response Maturity Assessment,
Report Number OIG-26-06

The U.S. Government Publishing Office, Office of the Inspector General, conducted an audit to assess the maturity of cybersecurity incident response capabilities for detection, analysis, and handling, Project Number A-2025-002.

We reported two findings and made three recommendations to improve cybersecurity incident response. We made no substantive changes to the final report from the draft report based on management's comments. We included a summary and an evaluation of management's comments on page 11, and the comments in their entirety in Appendix G. The planned corrective actions should resolve the issues identified in the report.

We appreciate the cooperation provided by your staff. If you have any questions or need additional information, please do not hesitate to contact Lori Lau Dillard, Assistant Inspector General for Audit, at llaudillard@gpo.gov or (202) 512-0318.

NATHAN J. DEAHL
Inspector General

RESULTS IN BRIEF

What We Did

GPO recognizes the critical importance of maintaining a robust cybersecurity posture to protect its systems and information assets. In alignment with its 2023–2027 Strategic Plan, GPO has prioritized cybersecurity as a core objective, entrusting the Agency Information Technology Services Business Unit with comprehensive risk management responsibilities.

The *Computer Security Incident Response Team Framework and Procedures* (CSIRT Framework) governs GPO's cybersecurity incident response efforts. GPO developed this framework using industry standards, particularly those of the National Institute of Standards and Technology (NIST). Also, while GPO is not required to comply with *Federal Information Security Modernization Act* (FISMA), management has adopted many of its standard practices and NIST recommendations.

The OIG Audit Division conducted an audit to assess the maturity of cybersecurity incident response using established FISMA Reporting Metrics. Our objective was to assess the maturity of cybersecurity incident response capabilities for detection, analysis, and handling.

What We Recommended

We made three recommendations to address the lack of detailed policies and procedures, inconsistent documentation of computer security incidents, and inaccurate records within the service ticketing system.

What We Found

Finding 1 Incident Detection and Analysis.

We found that GPO has established and communicated its policies and procedures for incident detection and analysis. However, the policy does not include procedures for handling different types of incidents and nor does it define a common set of categories to describe threats based on their characteristics, tactics, and potential impact. Additionally, we analyzed over 35,000 support system tickets and found that GPO did not consistently follow its own procedures for identifying, categorizing, and documenting its analysis for computer security incidents. Overall, we determined that GPO's incident detection and analysis processes generally align with the 'Defined' maturity level, as defined in FISMA Reporting Metrics.

Finding 2 Incident Handling.

We found that the CSIRT Framework provides guidance on incident handling and has expanded system recovery processes. Despite these improvements, the policy still lacks detailed containment strategies for different incident types and detailed eradication procedures. Based on FISMA Reporting Metrics, we found that GPO's incident handling processes currently reflect the 'Ad Hoc' maturity level.

GPO can improve incident response by tracking cybersecurity incidents with the new incident category, but tracking alone isn't enough. Incident tickets must include details such as the reasons for decisions and the actions taken during containment, eradication, and recovery to assess response effectiveness. Failing to include these details limits management's ability to improve the incident response plan. Additionally, capturing lessons learned from past incidents is vital for advancing maturity, ensuring accountability, and maintaining consistency.

Table Of Contents

INTRODUCTION

Objective

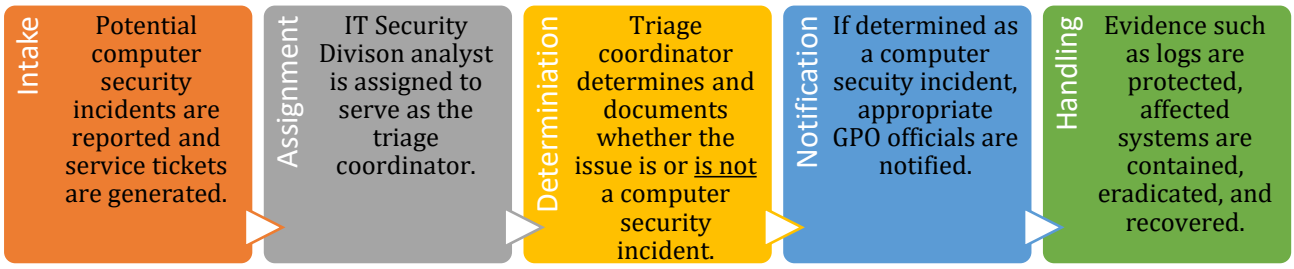
This report presents the results of our self-initiated audit of the U.S. Government Publishing Office's (GPO) cybersecurity incident response maturity assessment. (Project Number A-2025-002). Our objective was to assess the maturity of GPO's cybersecurity incident response capabilities for detection, analysis, and handling. See Appendix A for additional information about this audit.

Background

GPO recognizes the critical importance of maintaining a robust cybersecurity posture to protect its systems and information assets. In its 2023–2027 Strategic Plan, GPO identified maintaining a sound, acceptable cybersecurity posture as a core objective. The Agency Information Technology Services (AITS) Business Unit is charged with taking all necessary and appropriate action to ensure effective management of cybersecurity risk to GPO. Led by the Chief Information Officer and Chief Information Security Officer, this crucial responsibility is carried out by the Computer Security Incident Response Team (CSIRT) within the Information Technology (IT) Security Division. The CSIRT coordinates and executes GPO's computer security incident efforts.

A computer security incident response process begins when a user reports an issue by submitting a ticket in the service ticketing system. Alternatively, issues can be reported to IT Security Division employees via phone or email, who then generate a service ticket. An analyst from the IT Security Division is assigned as the CSIRT triage coordinator (triage coordinator) to analyze the issue and confirm whether it qualifies as a computer security incident. If the triage coordinator determines that the issue is a computer security incident, they will notify appropriate GPO officials. Concurrently, the triage coordinator handles the incident by securing evidence logs, containing and eradicating affected systems, and facilitating system recovery. The triage coordinator should record and document all actions taken during the incident response process in the service ticketing system. Figure 1 below shows the incident response process.

Figure 1. Computer Security Incident Response Process

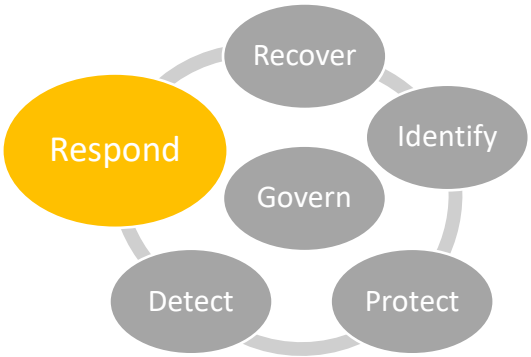


Source: OIG analysis based on GPO policy.

The policy governing GPO's computer security incident response efforts is encapsulated in the *CSIRT Framework and Procedures*[1] (CSIRT Framework). GPO developed this framework using industry standards, particularly the *National Institute of Standards and Technology's* (NIST) *Computer Security Incident Handling Guide* (NIST Special Publication 800-61). GPO also aligns its cybersecurity postures with relevant Presidential Executive Orders[2] (EO). Despite GPO being a Legislative Branch agency, its risk management decisions can impact national security, especially through programs such as passport operations; therefore, GPO seeks to adhere to federal best practices.

Originally enacted in 2002 and subsequently revised in 2014, the *Federal Information Security Modernization Act* (FISMA) requires Federal Executive Branch agencies to develop comprehensive programs to safeguard government information and systems against cyber threats, with an emphasis on risk management and the implementation of NIST-established standardized security controls. While GPO is not required to comply with FISMA, management has adopted many of its standard practices and NIST recommendations. As shown in Figure 2, the *NIST Cybersecurity Framework* (CSF) *2.0* of February 2024 has six core functions: Govern, Identify, Protect, Detect, Respond, and Recover.

Figure 2. NIST Cybersecurity Framework Core Functions



The *FY 2025 Inspector General FISMA Reporting Metrics* (FISMA Reporting Metrics) of April 2025 was developed in collaboration with the Office of Management and Budget, the Council of the Inspectors General on Integrity and Efficiency, and other stakeholders to evaluate the effectiveness of information security programs and practices. The FISMA Reporting Metrics align with the NIST CSF 2.0 six core functions and establish a five-level maturity model for assessing federal information security programs and practices. See Figure 3 below. We focused on evaluating GPO's maturity for the Respond function, encompassing incident detection and analysis, and incident handling.

[1] In this auditor's report, we based our assessment against the CSIRT Framework, version 1.6.13, issued in November 2024. During the audit, management updated its policy in December 2025 and issued CSIRT Framework, version 1.7. We've considered the CSIRT Framework, version 1.7, for assessing GPO's cybersecurity incident response maturity, where applicable.
[2] EO 13800 of May 2017, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* and EO 13833 of May 2018, *Enhancing the Effectiveness of Agency Chief Information Officers*.

Figure 3. Maturity Level Descriptions

Source: FISMA Reporting Metrics.

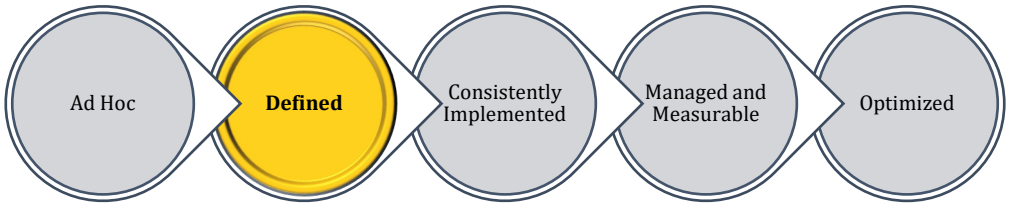
AUDIT RESULTS

Finding 1. Incident Detection and Analysis

We determined that GPO's incident detection and analysis processes generally align with the 'Defined' maturity level based on FISMA Reporting Metrics. According to these metrics, an organization reaches this level by defining and communicating policies and procedures but not consistently implementing them.

GPO has established and communicated policies and procedures within the CSIRT Framework. However, the policy lacked procedures for handling various incident types and a common taxonomy of attack vectors. The taxonomy of attack vectors refers to the classification and organization of different methods or pathways through which cyberattacks can occur. In addition, triage coordinators did not always document their analysis as required in the policy. Consequently, GPO has not consistently documented the analysis used to identify incidents, impacting their ability to accurately account for past security incidents and ensure proper incident response procedures. See Figure 4 below for the maturity rating and Appendix B for a summary of our assessment of incident detection and analysis.

Figure 4. GPO Maturity Rating for Incident Detection and Analysis



Source: OIG analysis.

Policies and Procedures

Our review of the CSIRT Framework revealed that, while it included a list of reportable incidents and threats, it lacked a common taxonomy of attack vectors and specific incident handling procedures for the detection and analysis phase. A taxonomy of attack vectors is a structured classification system that categorizes the methods and techniques that attackers use to exploit vulnerabilities and compromise computer systems and networks. For example:

- Email attack vectors utilize email to perpetrate an attack, such as through an attachment or a link to a malicious website.
- External media attack vectors use removable media or peripheral devices to implant malicious code.

According to NIST,[3] incidents can happen in numerous ways, making it impractical to specify step-by-step instructions for every case. Organizations should be prepared to handle any incident and focus on incidents involving common attack vectors to improve detection and response.

During our audit, GPO updated the CSIRT Framework in December 2025. As part of the update, the policy included an incident classification document, which resolved the lack of a common threat vector taxonomy. However, despite the addition of incident classification, specific incident handling procedures for the detection and analysis phase remained missing. See Appendix D for a list of changes between the CSIRT Framework version 1.6.13 and version 1.7.

Incident Documentation

GPO does not consistently document its determination of computer security incidents. According to the CSIRT Framework, at the end of the identification phase, the triage coordinator must determine whether the issue reported is:

- A problem to be resolved, but NOT a computer security incident.

  or

- A computer security incident, and the remainder of the CSIRT Framework will be executed.

Furthermore, the CSIRT Framework states, *"This determination and the text will be entered into the …ticket # by the CSIRT Triage Coordinator."*

While GPO updated the CSIRT Framework in December 2025, the new policy removed the requirement for the triage coordinator to document their determination and enter the text into the service ticket.

We analyzed over 35,000 tickets submitted in the service ticketing system from October 1, 2021, to July 11, 2025, and found only one ticket with a documented determination that it was not a computer security incident. The remaining tickets lacked this determination. Based on our analysis, we identified 56 tickets potentially related to computer security incidents and conducted inquiries with officials from the IT Security Division. Based on our inquiries, the officials acknowledged that 10 out of the 56 tickets were computer security incidents, as detailed in Table 1 below.

[3] *NIST Special Publication 800-61 Revision 2*, *Computer Security Incident Handling Guide*, August 2012, Section 3.2.1, Attack Vectors.

Table 1. Ten Computer Security Incidents Not Identified and Documented

Incident Number	Date Reported	Description
83005	7/7/2025	Trojan horse malware detected
82829	7/1/2025	Virus/malware detected
82443	6/16/2025	Malware detected
82358	6/12/2025	Malware detected
82036	5/30/2025	Malware detected
81411	5/6/2025	Malware detected
75531	10/24/2024	Malware detected
74584	9/26/2024	Pop-up scam alert
40647	3/22/2024	Website service degradation and defacement
58546	4/12/2023	Infected computer sending spam

Source: Service Ticketing System.

In 2024, the IT Security Division created the "Computer Security Incident" category within the service ticketing system. However, GPO has not consistently used this category correctly. Specifically, of the 10 incidents in Table 1, nine incidents occurred during or after 2024, but only one ticket, 40647, was classified under the "Computer Security Incident" category. Our review identified 17 additional tickets categorized as "Computer Security Incident." However, upon further inquiry, IT Security Division employees did not recognize any of these tickets as computer security incidents. According to the CSIRT Framework, incidents not confirmed as security incidents should be reclassified as "problem" tickets rather than computer security incidents. See Table 2 for the 17 tickets.

Table 2. 17 Tickets Not Recognized as Computer Security Incidents

Ticket Number	Date Reported	Description
52831	7/1/2025	Secure room found to be unlocked
52711	6/27/2025	System Test
51747	5/20/2025	Privacy Incident
51007	4/24/2025	Privacy Incident
50773	4/15/2025	Privacy Incident
48611	1/29/2025	Login attempts from multiple locations
48491	1/24/2025	Login attempts from multiple locations
48487	1/24/2025	Login attempts from multiple locations
47105	11/15/2024	Login attempts from multiple locations
47030	11/13/2024	Login attempts from multiple locations
46303	10/18/2024	Login from unknown user account
46264	10/16/2024	Login attempts from multiple locations
46158	10/11/2024	Login attempts from multiple locations
45524	9/24/2024	Phishing attempt
42633	6/14/2024	Malware detected
41496	4/29/2024	User received "Web Attack" notification
40776	3/30/2024	User received spam text message

Source: Service Ticketing System.

We analyzed the 17 tickets under the "Computer Security Incident" category in Table 2 and identified seven tickets involving multiple simultaneous logins from different locations by the same user, indicating unauthorized access attempts. See Table 3 below. According to the CSIRT Framework, such attempts, whether successful or not, are reportable computer security incidents. However, triage coordinators did not consider them incidents due to the unsuccessful access attempts, contrary to the CSIRT Framework.

Table 3. Login Attempts from Different Locations by a Single User

Ticket Number	Date Reported
48611	1/29/2025
48491	1/24/2025
48487	1/24/2025
47105	11/15/2024
47030	11/13/2024
46264	10/16/2024
46158	10/11/2024

Source: Service Ticketing System.

IT Security Division officials explained that many of their staff are relatively new to GPO. While some employees have held similar positions at other Federal agencies, they believed that there was a lack of institutional knowledge transfer. However, they are working to update cybersecurity policies and procedures.

Inconsistent identification of computer security incidents hampers management oversight. Without a consistent review process for declaring and documenting computer security incidents, management cannot ensure proper procedures are followed. Furthermore, GPO will have difficulty developing meaningful performance measures without a clear incident identification.

According to NIST,[4] the most difficult part of incident response is accurately detecting and evaluating potential incidents. The best approach is to 1) have skilled personnel, 2) follow a clear process, and 3) maintain detailed documentation.

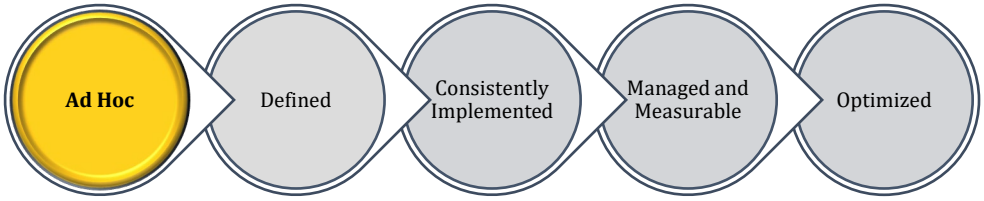
[4] *NIST Special Publication 800-61 Revision 2, Computer Security Incident Handling Guide*, August 2012, Section 3.2.4 Incident Analysis.

Finding 2. Incident Handling

We found that GPO's incident handling processes are generally at the 'Ad Hoc' maturity level as defined in the FISMA Reporting Metrics. This is due to the lack of detailed policies, procedures, and processes required to reach the 'Defined' maturity level, which demands comprehensive containment and eradication strategies for each key incident type.

While the updated December 2025 CSIRT Framework has expanded system recovery processes, the policy still lacks detailed containment strategies for different incident types and detailed eradication procedures. See Figure 5 below for the maturity rating and Appendix C for a summary of our assessment.

Figure 5. GPO Maturity Rating for Incident Handling



Source: OIG analysis.

Policies and Procedures

The CSIRT Framework outlines a 21-step process for responding to computer security incidents, from the initial identification to post-incident review. The containment process is covered in step 16 and eradication in step 17.

Containment
Step 16 addresses containment, the process of isolating the issue to prevent resource overload and minimize damage. The CSIRT Framework identifies several reportable incidents, such as 1) unauthorized access, 2) malicious code, 3) denial of service, 4) scans and probes, and 5) inappropriate usage. While it instructs the triage coordinator to take steps to contain the incident and document them in the service ticket, it lacks specific strategies for the different incident types.

NIST[5] recommends that organizations create specific containment strategies for each incident type to enable rapid decision-making during incidents. For instance, a strategy for an unauthorized access incident may call for disconnecting the impacted system from the network and disabling any user accounts used in the incident. In the case of malicious code incidents, NIST describes identifying and isolating infected host devices as a common containment strategy.

[5] *NIST Special Publication 800-61 Revision 2, Computer Security Incident Handling Guide*, August 2012. Specific examples of containment strategies are found in *NIST Special Publication 800-61 Revision 1,* March 2008.

Eradication
In step 17, after an incident is contained, the triage coordinator is tasked with eradicating the incident's source and documenting the steps taken in the service ticket. However, the framework provides limited detail, offering only one example for malicious code eradication as shown below.

> *"…systems may need to have the malicious software deleted in order to move to the recovery step later. The CSIRT Coordinator will so note in the* [*service ticketing system*] *actions required and taken to delete or remove malicious code or otherwise eliminate the cause of the incident."*

Our analysis of the 10 tickets in Table 1 revealed that, while all 10 generally described eradication steps (such as a virus scan or deleting files), only one ticket, 40647, included containment and recovery information. Furthermore, IT Security Division officials could only provide a draft after-action report for this ticket, which was not attached to the incident ticket in the service ticketing system. This particular report pertained to a significant incident involving the defacement of a public GPO website.

Without defined containment strategies, GPO risks greater damage during cybersecurity incidents, including extended downtime and loss of critical services. Clear guidance on isolating or stopping malicious activity is crucial to prevent a broader incident, extended downtime, loss of critical services, and increased difficulty in identifying compromised systems or data. Furthermore, the absence of strategies can lead to inconsistent decision-making under pressure, potentially resulting in financial and reputational damage.

Conclusion

GPO has the opportunity to enhance its incident response maturity, encompassing both incident detection and analysis, and incident handling. Establishing the "Computer Security Incident" category to track cybersecurity incidents is a step in the right direction. However, tracking alone addresses only the volume of incidents. Without including essential details in incident tickets—such as the rationale for the determination and the specific actions taken for containment, eradication, and recovery—the tickets fall short of providing meaningful insight into the effectiveness of the incident response capability. This lack of information limits management's ability to make informed decisions about improving the incident response plan and overall capability. Furthermore, thoroughly capturing and documenting lessons learned from previous cybersecurity incidents is crucial for advancing maturity, ensuring accountability, and promoting consistency in incident response processes.

Recommendations for the Director:

Recommendation 1: Update the CSIRT Framework and Procedures. Include detailed procedures for the following areas:

a. Handling specific incident types during the Detection and Analysis phase.
b. Incident containment strategies for incident types.
c. Incident eradication activities.

Recommendation 2: Ensure that Triage Coordinators fully document key information in the incident ticket, including (1) the determination of whether or not the event is a computer security incident and (2) the steps taken for incident containment, eradication, and recovery.

Recommendation 3: Ensure tickets identified in Tables 1 and 2 are correctly categorized as "Computer Security Incident" or reclassified as "problem" tickets in the service ticketing system.

MANAGEMENT'S COMMENTS

Management agreed with the findings and all recommendations. See Appendix G for management's comments in their entirety.

Regarding recommendation 1, management stated that they are developing standardized incident response procedures for managing common incident types during detection and analysis. These procedures will provide employees with clear guidance for reviewing alerts, identifying indicators, documenting evidence, and determining whether activity should be classified as a security event or escalated to a security incident. Management is also implementing supporting documentation within the incident management workflow to ensure analysts consistently document investigation steps, containment actions, eradication activities, and recovery efforts within incident tickets. The target implementation date (TID) is September 30, 2026.

Regarding recommendation 2, management stated that they will require employees to document key investigative details in incident tickets, including whether the activity is classified as a security event or a computer security incident, the analysis performed, the security tool indicators reviewed, and the evidence evaluated. Management will also update the service ticketing system workflow to require an after-action documentation report of the response actions taken during the containment, eradication, and recovery phases, to ensure investigation activities and response efforts are clearly recorded and traceable. The TID is September 30, 2026.

Regarding recommendation 3, management stated that due to technical limitations, closed tickets in the service ticketing system cannot be reopened after 72 hours. Therefore, the IT Security Division and Service Ticketing System Teams will collaborate on the appropriate solution to ensure that, when tickets identified in Tables 1 and are searched in the future, they appear as security incidents. Management will also ensure that guidance and training will be incorporated into operational procedures to ensure consistent classification decisions during triage and review moving forward. The TID is September 30, 2026.

EVALUATION OF MANAGEMENT'S COMMENTS

The OIG considers management's comments responsive to recommendations 1 through 3, and the planned corrective actions should resolve the issues identified in the report. All recommendations require OIG concurrence before closure. The OIG requests written confirmation when corrective actions are completed. All recommendations should not be closed until the OIG provides written confirmation that they can be closed.

APPENDICES

Appendix A. Objective, Scope, and Methodology

Our objective was to assess GPO's cybersecurity incident response capabilities for detecting, analyzing, and handling. Specifically, we assessed GPO's maturity using the *FY 2025 Inspector General FISMA Reporting Metrics,* within the Respond Function area, to determine to what extent GPO implemented processes related to 1) incident detection and analysis, and 2) incident handling.

To accomplish our objective, we:

- Reviewed applicable GPO policies and procedures related to computer security incident response, including the CSIRT Framework and Procedures.
- Reviewed NIST incident response standards.
- Interviewed key personnel, including the Chief Information Security Officer, Information Security Chief, and IT Security Division staff, to understand roles, responsibilities, and the use of detection technologies, including security information and event management (SIEM) tools and other monitoring solutions.
- Conducted walkthroughs of the incident response process, including service ticket creation and SIEM tools.
- Analyzed over 35,000 service tickets to identify those related to computer security incidents.

To determine the maturity ratings for GPO's computer security incident response program, we compared *GPO's CSIRT Framework and Procedures* to *NIST Special Publication 800-61, Revision 2, Computer Security Incident Handling Guide*. We then assigned a maturity rating based on the requirements in the *FY25 Inspector General FISMA Reporting Metrics,* within the Respond Function area.

To identify potential computer security incidents and evaluate incident response practices, we analyzed over 35,000 service tickets submitted between October 1, 2021, and July 11, 2025. We identified 56 tickets that appeared to involve security issues and provided them to GPO for validation. GPO confirmed that 10 of these tickets were actual computer security incidents. We then examined these 10 incidents in detail to evaluate how incident handling steps were executed and documented.

We also assessed whether CSIRT triage coordinators documented the determination of whether an event was a computer security incident in accordance with the CSIRT Framework requirements. We obtained access to the service ticketing system and reviewed the tickets for documentation of steps taken during the incident response process, including detection, analysis, and handling.

We conducted this performance audit from June 2025[6] through March 2026, 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 objective. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. We discussed our observations and conclusions with management on February 12, 2026, and March 4, 2026, and included their comments where appropriate.

Computer-Generated Data
We assessed the reliability of the data in the service ticketing system. We met with IT staff who managed the system and received a walkthrough of how users enter data into tickets and how IT staff review them and record their work. We observed IT staff export a ticket report and confirmed that all tickets were included in the report. We found no data reliability issues and concluded that the data were sufficiently reliable for the purposes of this report.

Internal Controls
We assessed internal controls and compliance with laws and regulations necessary to satisfy the audit objective.

Prior Audit Coverage
The OIG did not identify any prior audits related to the audit objective within the last five years.

[6] Due to the lapse of government funding, audit work was paused from October 1 through November 12, 2025.

Appendix B. OIG Maturity Assessment Summary - Incident Detection and Analysis

Maturity Level	FY 2025 Inspector General FISMA Reporting Metrics	OIG Assessment		
		Meets	Partially Meets	Does not meet
Level 1: Ad Hoc	The Agency has not defined and communicated its policies, procedures, and processes for incident detection and analysis. In addition, the organization has not defined a common threat vector taxonomy for classifying incidents and its processes for detecting, analyzing, and prioritizing incidents.			☑
Level 2: Defined	The Agency has defined and communicated its policies, procedures, and processes for incident detection and analysis.	☑		
	The Agency has defined a common threat vector taxonomy and developed handling procedures for specific types of incidents, as appropriate. Note 1		☑	
	The Agency has defined its processes and supporting technologies for detecting and analyzing incidents, including the potential adverse events and indicators, and how they are generated and reviewed, and for prioritizing incidents. Note 1	☑		
Level 3: Consistently Implemented	The Agency consistently uses its enterprise-wide threat vector taxonomy to classify incidents and consistently implements its processes for incident detection, analysis, and prioritization.			☑
	The Agency consistently implements and analyzes potential adverse events and indicators generated by, for example, the following enterprise-wide technologies: intrusion detection/ prevention, security information and event management (SIEM), antivirus and antispam software, and file integrity software.	☑		
	The Agency consistently captures and shares lessons learned on the effectiveness of its incident detection policies and procedures, and makes updates as necessary.			☑
	The Agency is meeting event logging requirements at the basic maturity level in accordance with the Office of Management and Budget requirements. Note 2	☑		
Level 4: Managed and Measured	The Agency monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its incident detection and analysis policies and procedures.			☑
	The Agency ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format.			☑
	The Agency uses profiling techniques to measure characteristics of expected activities on its networks and systems so that it can more effectively detect security incidents.			☑

Maturity Level	FY 2025 Inspector General FISMA Reporting Metrics	OIG Assessment		
		Meets	Partially Meets	Does not meet
	The Agency is meeting event logging requirements at the intermediate level in accordance with the Office of Management and Budget requirements.[Note 2]	☑		
Level 5: Optimized	The Agency is making demonstrated progress towards implementing event logging requirements at the advanced level in accordance with the Office of Management and Budget requirements.			☑

Note 1: Assessment based on updated *CSIRT Framework and Procedures* version 1.7.
Note 2: Our conclusion for event logging was based on GPO's self-assessment on whether GPO is meeting the logging requirements. The OIG did not validate GPO's response.

Appendix C. OIG Maturity Assessment Summary - Incident Handling

Maturity Level	FY 2025 Inspector General FISMA Reporting Metrics	OIG Assessment		
		Meets	Partially Meets	Does not meet
Level 1: Ad Hoc	The Agency has not defined its policies, procedures, and processes for incident handling to include containment strategies for various major incidents, eradication activities to eliminate components of an incident and mitigate any vulnerabilities that were exploited, and recovery of systems.	☑		
Level 2: Defined	The Agency has defined and communicated its policies, procedures, and processes for incident handling to include containment strategies for each key incident type.			☑
	In developing strategies, the Agency takes into consideration: the potential damage to and theft of resources, the need for evidence preservation, service availability, time and resources needed to implement the strategy, effectiveness of the strategy, and duration of the solution.			☑
	The Agency has defined its processes to eradicate components of an incident, mitigate any vulnerabilities that were exploited, and recover system operations.			☑
Level 3: Consistently Implemented	The Agency consistently implements an enterprise-wide incident handling policies, procedures, containment strategies, and incident eradication processes.			☑
	The Agency consistently implements enterprise-wide processes to remediate vulnerabilities that may have been exploited on the target system(s) and recovers system operations.			☑
	The Agency is consistently capturing and protecting incident data and metadata at an enterprise-wide level, sharing lessons learned on the effectiveness of its incident handling policies and procedures, and making updates as necessary.			☑
Level 4: Managed and Measured	The Agency monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its incident handling policies and procedures.			☑
	The Agency ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format.			☑
	The Agency manages and measures the impact of successful incidents and can quickly mitigate related vulnerabilities on other systems so that they are not subject to exploitation of the same vulnerability.			☑
Level 5: Optimized	The Agency uses dynamic reconfiguration (e.g., changes to router rules, access control lists, and filter rules for firewalls and gateways) to stop attacks, misdirect attacks, and isolate component systems.			☑

Appendix D. CSIRT Framework and Procedures Comparison

The comparison table highlights key differences between *CSIRT Framework and Procedures* versions 1.6.13 and 1.7.

Category	Version 1.6.13[7]	Version 1.7	Key Difference
Roles & Responsibilities	Not defined.	Breakdown of roles.	Roles and responsibilities are clarified.
Detection Tools	Not defined.	Examples of detection tools to assist in detecting incidents.	Adds supporting technology for threat detection.
Incident Classification	Three levels: High, Moderate, and Low.	Four levels: Critical, High, Medium, Low, with examples.	Adds prioritization based on various factors noted in the levels.
Notification Procedures	All parties noted are to be contacted.	Specific contact chains and escalation protocols based on incident classification.	Contacts listed are notified based on the incident classification level.
Containment & Eradication	Basic overview of stopping or isolating systems. No additional detailed steps.	Mitigation tools assist in containment and eradication.	Adds cybersecurity practices.
Recovery Process	Overview of steps to rebuild and restore systems.	Recovery process using Incident handling technical rules.	Adds cybersecurity practices.
Lessons Learned	After an Incident closed. A post-incident review meeting within 1 week.	After an incident has closed, a post-incident meeting is held within the 4-week review period. For any high, critical, or incident involving criminal activity, a technical and executive report is prepared.	Delayed review period by another 3 weeks.

[7] GPO issued *CSIRT Framework and Procedure version 1.6.14* in June 2025. Changes were minimal from version 1.6.13. The contact list was updated due to new personnel.

Appendix E. Table of Recommendations

Recommendation	Management Response	Status	Return on Investment
1. Develop detailed procedures for the following areas: a. Handling specific incident types during the Detection and Analysis phase b. Incident containment strategies for major incident types c. Incident eradication activities	Concur. TID is September 30, 2026.	Open	Nonmonetary – Improve processes and management controls. By implementing this recommendation, GPO can update policies to improve operational effectiveness and efficiencies in its computer security incident response program. This will allow GPO to better identify computer security incidents and ensure that staff perform proper actions to quickly resolve them with minimal damage to GPO systems.
2. Develop procedures to ensure that Triage Coordinators fully document key information in the incident ticket, including (1) the determination of whether or not the event is a computer security incident and (2) the steps taken for incident containment, eradication, and recovery.	Concur. TID is September 30, 2026.	Open	Nonmonetary – Improve processes and management controls. By implementing this recommendation, GPO can update procedures to improve the documentation of computer security incident response actions. This will enable improved management oversight and performance measurement.
3. Ensure tickets identified in Tables 1 and 2 are correctly categorized as "Computer Security Incident" or reclassified as "problem" tickets in the service ticketing system.	Concur. TID is September 30, 2026.	Open	Nonmonetary – Improve compliance. Implementing this recommendation will ensure accurate data when accounting for incidents in the future.

Appendix F. Abbreviations

AITS	Agency Information Technology Services
CSF	Cybersecurity Framework
CSIRT	Computer Security Incident Response Team
EO	Executive Order
FISMA	Federal Information Security Modernization Act
FY	Fiscal Year
GPO	Government Publishing Office
IT	Information Technology
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
SIEM	Security Information and Event Management
TID	Target Implementation Date

Appendix G. Management's Comments

Management's comments, in their entirety, are presented on the next three pages.

HUGH NATHANIAL HALPERN
Director

GPO

MEMORANDUM

Date: March 26, 2026

To: Inspector General

Subject: Response to DDR Cybersecurity Incident Response Maturity Assessment – Memorandum OIG-26-018

Thank you for the opportunity to offer the Agency's response to the OIG Cybersecurity Incident Response Maturity Assessment, Project Number A-2025-002.

In General

The Government Publishing Office (GPO) recognizes the importance of further developing and formalizing detailed procedures across the detection and analysis phases, as well as enhancing guidance related to containment strategies and eradication activities. In response, we are making improvements to ensure triage coordinators consistently document key investigative information in incident tickets, including clearly identifying whether alerts are security events or security incidents, documenting the analysis performed, and capturing actions taken for containment, eradication, and recovery.

Additionally, we are strengthening processes to ensure tickets are consistently classified into appropriate categories and prioritized based on established criteria, and that we document investigation details to support accurate tracking, reporting, and effective incident response. These enhancements will be supported through updates to the ServiceNow incident management module to improve the consistency and visibility of investigation activities and response actions.

Agency Response to Recommendations in the Report

Recommendation 1

Develop detailed procedures for the following areas:

a. Handling specific incident types during the Detection and Analysis phase
b. Incident containment strategies for major incident types
c. Incident eradication activities

GPO concurs with this recommendation.

The Agency acknowledges the importance of creating detailed procedures to ensure consistent incident response activities. To fulfill this recommendation, the organization is developing standardized incident response playbooks that outline procedures for managing common incident types during detection and analysis. These playbooks will provide analysts with clear guidance for reviewing alerts, identifying indicators,

documenting evidence, and determining whether activity should be classified as a security event or escalated to a security incident.

The playbooks will detail recommended containment strategies, such as segmenting networks, blocking malicious Internet Protocol (IP) addresses, disabling compromised accounts, and physically disconnecting infected devices as needed. Eradication activities may involve removing the root cause of a breach, eliminating malicious components (like malware and rogue accounts), and closing vulnerabilities to prevent re-entry across major incident categories, ensuring consistent response actions.

We are also implementing supporting documentation within the incident management workflow to ensure analysts consistently document investigation steps, containment actions, eradication activities, and recovery efforts within incident tickets.

The Agency expects to complete the documentation by the end of September 2026.

Recommendation 2

Ensure that Triage Coordinators fully document key information in the incident ticket, including (1) the determination of whether or not the event is a computer security incident and (2) the steps taken for incident containment, eradication, and recovery.

GPO concurs with this recommendation.

To address this recommendation, Triage Coordinators will be required to document key investigative details in incident tickets, including whether the activity is classified as a security event or a computer security incident, the analysis performed, the security tool indicators reviewed, and the evidence evaluated.

Process enhancements to the ServiceNow ticketing workflow will help ensure these documentation requirements are consistently captured and maintained. Incident tickets will include an after-action documentation report of the response actions taken during the containment, eradication, and recovery phases, to ensure investigation activities and response efforts are clearly recorded and traceable.

The Agency expects to complete this recommendation by September 2026.

Recommendation 3

Ensure tickets identified in Tables 1 and 2 are correctly classified in the IT ServiceHUB.

GPO concurs with this recommendation.

The security team will work with the ServiceNow team to find the best way to properly categorize the identified tickets. However, due to technical limitations, closed tickets cannot be reopened after 72 hours. Therefore, the team will determine the appropriate solution to ensure that, when these tickets are searched in the future, they appear as security incidents. Additional guidance and training will be incorporated into operational procedures to ensure consistent classification decisions during triage and review moving forward.

The Agency expects to complete this recommendation by the end of September 2026

Thank you for the opportunity to provide the Agency's input on these recommendations. The Agency spent approximately six hours preparing this response. If you have any questions, please contact me.

HUGH NATHANIAL HALPERN

cc: **Deputy Director**
Chief of Staff
General Counsel