Office of Inspector General
U.S. Government Accountability Office

# INFORMATION SECURITY

## Privacy Program Improvements Could Enhance GAO Efforts to Protect Data and Systems

March 2022
OIG-22-2

# Office of Inspector General
# U.S. Government Accountability Office
# Report Highlights

**March 31, 2022**

# INFORMATION SECURITY

## Privacy Program Improvements Could Enhance GAO Efforts to Protect Data and Systems

### Objective

This report presents the OIG's Fiscal Year (FY) 2021 assessment of the effectiveness of GAO's information security program in relation to selected Federal Information Security Modernization Act of 2014 (FISMA) requirements.

### What OIG Found

We assessed GAO's information systems against selected FY 2021 Inspector General (IG) FISMA reporting metrics, and found certain aspects pertaining to management of data protection and privacy have opportunities for improvement. While GAO has taken steps to protect sensitive information and prevent data exfiltration, opportunities exist to improve its privacy program in the areas of incident response and training for people with specific roles.

- GAO's Incident Response plan does not contain all the recommended elements for addressing incidents involving Personally Identifiable Information (PII). Specifically, the current GAO incident response procedures do not contain documented procedures for assessing the potential damage to organizations and individuals resulting from the loss of PII.
- All GAO employees and contractors receive privacy training annually, as part of a mandatory course on security and privacy awareness. However, we found that training for personnel with role-specific responsibility for PII has not been consistently implemented.

During a penetration test we performed to assess the effectiveness of controls in the configuration management and information security continuous monitoring categories, we did not identify any significant vulnerabilities that would result in substantial compromise. We also found that GAO's policies and procedures for security training and its approach to identity and access management generally align with NIST guidance.

### What OIG Recommends

We recommend that the Comptroller General direct the Chief Administrative Officer to direct the appropriate office(s) to (1) define and implement policies and procedures for incident response that align with NIST guidance for assessing privacy impact incidents and (2) define and implement policies and procedures for role-based privacy training which (a) identify who must regularly take the training, and (b) ensure annual compliance with such training. GAO agreed with the recommendations and outlined planned actions to address them.

March 31, 2022

**To:** Gene L. Dodaro
Comptroller General of the United States

**From:** L. Nancy Birnbaum
Inspector General

**Subject:** Transmittal of Office of Inspector General's (OIG) Audit Report

Attached for your information is our report, Information Security: Privacy Program Improvements Could Enhance GAO Efforts to Protect Data and Systems (OIG-22-2). The audit objective was to evaluate the extent to which GAO has complied with select Federal Information Security Modernization Act of 2014 (FISMA) requirements.

The report contains two recommendations aimed at improving GAO's privacy training and incident response. GAO agreed with our recommendations. Management comments are included in Appendix II of our report. Actions taken in response to our recommendations are expected to be reported to our office within 60 days.

We are sending copies of this report to the other members of GAO's Executive Committee, GAO's Congressional Oversight Committees, GAO's Audit Advisory Committee, and other GAO managers, as appropriate. The report is also available on the GAO website at https://www.gao.gov/ig and https://www.oversight.gov/reports, maintained by the Council of Inspectors General on Integrity and Efficiency.

If you have questions about this report, please contact me at (202) 512-9355 or birnbauml@gao.gov.

Attachment

cc: Edda Emmanuelli Perez, General Counsel
Karl Maschino, Chief Administrative Officer/Chief Financial Officer
Orice Williams Brown, Chief Operating Officer
Terrell Dorn, Managing Director, Infrastructure Operations
Howard Williams, Jr. Managing Director, Information Systems and Technology Services
Paul Johnson, Deputy Chief Administrative Officer
William Anderson, Controller/Deputy Chief Financial Officer
Adebiyi Adesina, Special Assistant to the Controller
Jennifer Ashley, Special Assistant for Operational Initiatives

## Table of Contents



## Tables

**Abbreviations**

| | |
|---|---|
| ARM | Applied Research and Methods |
| CIGIE | Council of the Inspectors General on Integrity and Efficiency |
| DHS | Department of Homeland Security |
| FISMA | Federal Information Security Modernization Act of 2014 |
| HCO | Human Capital Office |
| IO | Infrastructure Operations |
| ISTS | Information Systems and Technology Services |
| NIST | National Institute of Standards and Technology |
| PII | Personally Identifiable Information |

## Introduction

GAO relies extensively on information systems and technology to fulfill its mission and support related administrative needs. Strong information security controls reduce risks to information systems, the data they contain, and the people and processes they support. GAO systems must maintain effective information security controls to avoid being compromised, potentially resulting in damage to the organization, national security, or individual privacy.

GAO's Office of Inspector General (OIG) periodically assesses GAO's compliance with Federal Information Security Modernization Act of 2014[1] (FISMA) requirements. This report presents the results of the OIG's assessment for Fiscal Year (FY) 2021.

## Objective, Scope, and Methodology

We measured GAO's performance against selected FY 2021 Inspector General (IG) FISMA reporting metrics. These metrics were developed by the Council of the Inspectors General on Integrity and Efficiency (CIGIE), and the Department of Homeland Security (DHS), and other stakeholders, based on National Institute of Standards and Technology (NIST) requirements for executive branch agencies. We chose five FISMA reporting metrics in the "protect and detect" functional areas to review: (1) configuration management, (2) identity and access management; (3) data protection and privacy; (4) security training; and (5) information security continuous monitoring.[2] We selected these specific metrics using a risk-based approach, taking into account prior OIG work and other factors. We did not review other reporting metrics, such as risk management, supply chain risk management, and contingency planning, nor did we assess the maturity of GAO's information security against the selected reporting metrics.

To assess GAO's performance, we analyzed the agency's information security policies, procedures, and guidance. We also interviewed staff and analyzed information obtained from both GAO's Information Systems and Technology Services (ISTS) and Infrastructure Operations (IO) teams. We also considered other security-related work in planning and performing our audit, as appropriate. Additional information on our scope and methodology is presented in appendix I.

We conducted this performance audit from February 2021 through February 2022 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 that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

---

[1]Pub. L. No. 113-283, Dec. 18, 2014.

[2]Under NIST guidance, "protect" functions focus on developing and implementing appropriate safeguards to ensure delivery of critical services. NIST describes "detect" functions as those that focus on developing and implementing appropriate activities to identify the occurrence of a cybersecurity event. U.S. Department of Homeland Security, *National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity, (Gaithersburg, MD.: April 16, 2018).*

## Background

Congress has long recognized the importance of ensuring the security of federal information systems. In 2002, Congress passed the Federal Information Security Management Act[3] (FISMA 2002) which laid out responsibilities for executive branch agencies, including requiring each agency to develop, document, and implement an agency-wide information security program to support the operations and assets of the agency, using a risk-based approach to information security management. The act also assigned to NIST the responsibility for developing standards and guidelines that include minimum information security requirements. Additionally, the Office of Management and Budget (OMB) publishes guidance for executive branch agencies on implementing the NIST requirements.

To update FISMA 2002, recognizing changes that had occurred in the information security landscape, Congress passed the Federal Information Security Modernization Act of 2014 (FISMA),[4] which included additional provisions for executive branch agencies such as defining OMB and DHS reporting requirements.

NIST developed a risk management framework[5] to improve information security, strengthen risk management processes, and encourage the mutual acceptance of security assessment results among organizations. The risk framework promotes the development of security and privacy capabilities for information systems throughout their development life cycles. NIST recommends that organizations implement continuous monitoring processes to capture the current status of security and privacy controls over information systems; and to provide that information to senior leaders and executives for use in decisions on risk strategies for their organizational operations and assets.

NIST also developed the *Framework for Improving Critical Infrastructure Cybersecurity*,[6] which provides a framework to help organizations align policy requirements, business needs, and technological methodologies for cybersecurity risk management. CIGIE and executive branch agencies responsible for federal cybersecurity aligned the cybersecurity framework's metrics for assessing agency progress in implementing FISMA with the risk framework.[7] The FY 2021 metrics built on the work begun in FY 2016, when the IG FISMA

[3]FISMA 2002 was enacted as title III, E-Government Act of 2002, Pub L. No. 107-347, Dec. 17, 2002.

[4]The Federal Information Security Modernization Act of 2014 (Pub. L. No. 113-283, Dec. 18, 2014) largely superseded the Federal Information Security Management Act of 2002 (FISMA 2002), enacted as Title III, E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002). As used in this report, FISMA refers to the new requirements in FISMA 2014, and to other relevant FISMA 2002 requirements that were unchanged by FISMA 2014 and continue in full force and effect.

[5]National Institute of Standards and Technology, *Managing Information Security Risk: Organization, Mission, and Information System View*, SP 800-39 (Gaithersburg, MD: March 2011), developed in partnership with the Department of Defense, the Office of the Director of National Intelligence, and the Committee on National Security Systems.

[6]National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity* (Gaithersburg, MD: Feb. 12, 2014).

[7]The FY 2021 IG FISMA Reporting Metrics were developed as a collaborative effort amongst OMB, DHS, and the Council of the Inspectors General on Integrity and Efficiency (CIGIE), in consultation with the Federal Chief Information Officer (CIO) Council and other stakeholders.

reporting metrics were aligned with the five function areas in the risk framework: Identify, Protect, Detect, Respond, and Recover.

Table 1 describes how the five selected IG FISMA reporting metrics align with the NIST Cybersecurity Framework.

**Table 1: Selected Cybersecurity Framework Core Functions, Categories and Descriptions**

| IG FISMA Reporting Metric | NIST Cybersecurity Framework Category and Function | | Description |
|---|---|---|---|
| | Category | Function | |
| Configuration Management | Protect | Information Protection Processes and Procedures | Security policies, processes, and procedures are maintained and used to manage protection of information systems and assets. |
| Data Protection and Privacy | Protect | Data Security | Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information. |
| Identity and Access Management | Protect | Identity Management and Access Control | Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions. |
| Security Training | Protect | Awareness and Training | The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements. |
| Information Security Continuous Monitoring | Detect | Security Continuous Monitoring | The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures. |

Source: NIST Framework for Improving Critical Infrastructure Cybersecurity. | OIG-22-2

Although GAO, as a legislative branch agency, is not subject to FISMA, NIST or OMB guidance, its management has voluntarily aligned its security program with executive branch best practices, such as FISMA and NIST's cybersecurity framework.

## Privacy Program Improvements Could Enhance GAO Efforts to Protect Data and Systems

We assessed GAO's information systems against selected IG FISMA reporting metrics, and found certain aspects pertaining to data protection and privacy management have opportunities for improvement. While GAO has taken steps to protect sensitive information and prevent data exfiltration, opportunities exist to improve its privacy program in the areas of incident response and training for people with specific roles. During a penetration test we performed to assess the effectiveness of controls in the configuration management and information security continuous monitoring categories, we did not identify any

significant vulnerabilities that would result in substantial compromise. We also found that GAO's policies and procedures for security training and its approach to identity and access management generally align with NIST guidance.

### Aspects of GAO's Data Protection and Privacy Controls Could Be Strengthened

GAO has a process in place to protect sensitive data that resides on its network, and its privacy program policies and procedures generally align with NIST guidance. However, we identified improvements for incident response and role-specific privacy training. Specifically, NIST SP 800-53 revision 5 includes developing policies to define the organizational privacy program, taking steps to identify sensitive data leaving the network, and ensuring that individuals with access to PII understand their roles and responsibilities. Table 2 below details how we assessed GAO's privacy program against NIST recommendations.

**Table 2: OIG Assessment of GAO's Policies and Procedures Alignment with Recommended Privacy Program Elements**

| Privacy Program Program Element | OIG Assessment |
|---|---|
| Processes for conducting Privacy Impact Assessments (PIAs)[8] | ● |
| Requirements for contractors processing PII | ● |
| Plans for eliminating unnecessary PII holdings | ● |
| A framework for measuring annual performance goals and objectives for implementing identified privacy controls | ● |
| Actions to prevent or limit the exfiltration of sensitive data | ● |
| Privacy incident response policies and procedures | ◐ |
| Privacy Training and Awareness Requirements | ◐ |

● – GAO policies and procedures generally align with recommended practices

◐ – GAO policies and procedures do not fully align with recommended practices

Source: OIG Analysis of GAO Data. | OIG-22-2

We found that GAO had developed and implemented a process for performing PIAs, established requirements for contractors processing PII, communicated plans for eliminating unnecessary PII, and reported on annual performance goals for implementing privacy controls. However, GAO's policies and procedures specific to privacy incident response and training for individuals with special access to PII could be better defined and documented.

[8]A Privacy Impact Analysis is a process where an organization assesses how information is handled to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; determines the risks and effects of creating, collecting, using, processing, storing, maintaining, disseminating, disclosing, and disposing of information in identifiable form in an electronic information system; and examines and evaluates protections for handling information to mitigate potential privacy concerns.

GAO Should Enhance Incident Response Policies and Procedures

GAO's Incident Response plan does not contain all the recommended elements for addressing incidents involving PII. Specifically, the current GAO incident response procedures do not contain documented procedures for assessing the potential damage to organizations and individuals resulting from the loss of PII. NIST SP 800-53 revision 5 recommends that agencies develop and implement an incident response plan that includes:

- a process to assess whether PII or other sensitive data was impacted during a breach so that individuals or other organizations, including oversight organizations, can be contacted as needed;
- a process to assess whether PII or other sensitive data impacted during a breach would cause harm, embarrassment, inconvenience, or unfairness to affected individuals and determine what mechanisms to deploy to mitigate such harms; and
- identification of applicable privacy requirements.

GAO's existing directive[9] on information security has provisions for determining whom to notify in the event of an information security incident, including those involving PII, and contains provisions requiring employees to promptly report incidents. However, the current policies and procedures do not establish a risk assessment process to determine the full impact from incidents resulting in the loss of PII or sensitive data. According to GAO's records and privacy officials[10], the GAO Information Security Incident Response Team[11] performs some but not all of these risk assessment functions. For example, the information security incident response directive[12] does not document the process for assessing damage to individuals and organizations. Incident response policies and procedures that include all of the recommended elements for addressing incidents involving PII would help to ensure that GAO responds appropriately to privacy incidents.

GAO's Program for Individuals Who Require Role-Specific Privacy Training Requires Additional Definition

All GAO employees and contractors receive privacy training annually, as part of a mandatory course on security and privacy awareness. However, we found that training for personnel with role-specific responsibility for PII has not been consistently implemented. NIST SP 800-53 revision 5 recommends that agencies develop, implement, and update a comprehensive training and awareness strategy aimed at ensuring that personnel whose positions require special access to PII understand privacy responsibilities and procedures. This includes offering targeted, role-based privacy training for personnel having responsibility for PII or for activities that involve PII, on an annual basis.

While GAO offers privacy awareness training to groups of GAO employees with special access to or responsibility for PII, the training is offered only when requested and

[9]GAO Directive 0910.1-08

[10]GAO's Infrastructure Operations (IO) group is responsible for records and privacy. The IO Managing Director serves as GAO's Chief Privacy Officer.

[11]The GAO Information Security Incident Response Team is composed of the Chief Information Officer, the Chief Privacy Officer, the Director of ISTS Information Systems Security Group (ISSG); the Director of ISTS Customer Service; the Director of IO Records and Privacy; the Director of IO Facilities and Property Management (FPM); and the Director of IO Office of Security (OS).

[12]GAO Directive 0910.1-08

scheduled by a mission team. Since 2019, GAO has offered role-specific training to four groups of GAO personnel. These individuals in the Human Capital Office (HCO), Applied Research and Methods (ARM), information system business owners, and Record Liaison Officers all were identified as having increased access to PII and therefore needed additional training. However, two of these groups, HCO and ARM, received no training in fiscal year 2021 because they did not request it. For the other two groups, information system business owners and Record Liaison Officers, training was offered but GAO did not ensure that all personnel had taken it. Table 3 details the training offered each year by mission team.

**Table 3: Role-Specific Training Offered Each Year**

| Group | 2021 Training Provided | Training Dates |
|---|---|---|
| Applied Research and Methods | No | Last provided June 27, 2019 |
| Human Capital Office | No | Last provided February 27, 2020 |
| System Business Owners | Yes | Various dates in 2021 |
| Record Liaison Officers | Yes | Various dates in June, 2021 |

Source: OIG Analysis of agency data. | OIG-22-2

As a result, new employees of those groups and other individuals who have not taken the training may not fully understand their responsibilities and the potential consequences for the loss of PII under their control.

### OIG Penetration Test Did Not Identify Any Substantial Vulnerabilities in Configuration Management and Information Security Continuous Monitoring

We conducted a penetration test of internet-connected systems to assess potential vulnerabilities. We did not identify any significant vulnerabilities during the penetration test that would result in substantial compromise, but we did note some opportunities for GAO to improve its security posture. We shared the details of these potential vulnerabilities with GAO management in a separate communication for their review and action.

### GAO's Security Training; Identity and Access Management Programs Align with NIST Guidance

We found that the portions of GAO's identity and access management program we reviewed generally aligned with NIST guidance. Further, GAO effectively ensures that employees take security awareness training as required by policy.

NIST SP 800-53 revision 5 recommends that agencies develop policies and procedures to issue credentials, such as user identifiers and passwords, and take steps to ensure that users are aware of unacceptable utilizations of systems. Executive branch agencies generally use a comprehensive model that includes policy, strategy, processes, and technology to ensure that the right individual can access the right resource, at the right time, for the right reason in support of federal business objectives.

Although GAO does not use a traditional model, its policies and procedures effectively manage the creation and management of user access to systems and data. According to the Director of the Information Systems and Security Group, GAO does not use a traditional model because the guidance is largely focused on executive branch agencies. GAO's information technology guidelines establish rules of behavior that inform users

about unacceptable utilization of GAO systems and ensure that users are aware of the rules of behavior. These rules of behavior are communicated through access agreements for users. The rules of behavior define acceptable utilization of information technology resources at GAO, required authentication mechanisms, and connection requirements.

Additionally, GAO's policies and procedures are operating effectively to ensure that employees and contractors take its annual security awareness training. NIST SP 800-53 revision 5 recommends that organizations provide basic levels of information security literacy training to system users, which include measures to test users' knowledge level and policies and procedures to enable training delivery. GAO's Security and Awareness training for Fiscal Year 2021 and the order mandating users take this training meet these criteria.

## Conclusions

GAO's mission requires it to collect and store data on a variety of government programs, which makes it an attractive target for malicious actors. Security threats continue to evolve and become more sophisticated. Further, the speed at which new attack techniques become widely available, even to unsophisticated threat actors, underscores the need for GAO to continually improve its information security program. Generally, for the areas that we reviewed, GAO has established policies and procedures that are consistent with a NIST-aligned security program. However, GAO's privacy program could better define policies and procedures for assessing privacy impacts during incident response and for delivering training to individuals with access to PII.

## Recommendations for Executive Action

We recommend that the Comptroller General direct the Chief Administrative Officer to direct the appropriate office(s) to:

1. Define and implement policies and procedures for incident response that align with NIST guidance for assessing privacy incident impacts.
2. Define and implement policies and procedures for role-based privacy training which (a) identify who must regularly take the training, and (b) ensure annual compliance with such training.

## Agency Comments and Our Evaluation

The Inspector General provided GAO with a draft of this report for review and comment. In its written comments, reprinted in appendix II, GAO agreed with our recommendations and outlined planned actions to address them.

## Appendix I: Objective, Scope, and Methodology

We measured GAO's performance against select FY21 IG FISMA reporting metrics which are developed by Council of the Inspectors General on Integrity and Efficiency (CIGIE) and the Department of Homeland Security based on NIST requirements for executive branch agencies.[13] The FISMA reporting metrics are from the protect and detect functions and include: (1) configuration management; (2) identity and access management; (3) data protection and privacy; (4) security training; and (5) information security continuous monitoring. We selected these specific metrics, using a risk-based approach, taking into account prior OIG work and other factors. We did not review other reporting metrics, such as risk management, supply chain risk management, and contingency planning, nor did we assess the maturity of GAO's information security against the selected reporting metrics.

To assess GAO's performance, we analyzed the agency's information security policies, procedures, and guidance. We also interviewed staff and analyzed information obtained from both GAO's Information Systems and Technology Services (ISTS) and Infrastructure Operations (IO) teams. To assess the reliability of the data provided by GAO we reviewed it for missing information, outliers, or obvious errors. We also discussed the data with knowledgeable agency officials, and compared it to other sources, where available.

To assess GAO's identity and access management, we reviewed GAO's policies and procedures regarding user provisioning at GAO, access agreements, privileged and non-privileged authentication mechanisms, and connection requirements for remote access users.

To assess GAO's efforts regarding data protection and privacy, we reviewed GAO's policies and procedures for providing security awareness training. Additionally, we reviewed systems that GAO uses to detect and prevent the exfiltration of sensitive data from the network. Further, we reviewed policies and procedures for responding to the loss of PII. We interviewed program managers to understand any issues we identified.

To assess GAO's approach to security training, we reviewed GAO's policies and procedures, including implementation, of its security training course. We also reviewed the steps GAO takes to ensure that all employees have received security training and that appropriate employees have taken specialized security training, including monitoring reports and communicating about these efforts as appropriate.

As part of our assessment of GAO's configuration management and information security continuous monitoring, we performed a penetration test for GAO's internet-connected systems. The purpose of the penetration test was to determine the extent to which GAO's network and external or public facing applications are vulnerable to compromise through cyberattacks. We conducted testing between June 10th and June 21st, 2021, using tools and information that are publicly available, in accordance with the GAO OIG Rules of

[13]U.S. Department of Homeland Security, *FY 2021 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metric*s, (May 12, 2021).

Engagement.[14] We also reviewed available source code to look for application vulnerabilities.[15]

We conducted this performance audit from February 2021 through February 2022 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 objectives.

[14]The Rules of Engagement establish the necessary guidelines to execute the penetration test and vulnerability assessment. They document the scope, methodology, as well as data management and communications plan for the OIG's assessment of GAO systems.

[15]In order to avoid potential disruption to GAO operations, the OIG determined that it would not use attack methods such as Denial of Service and password brute-forcing to compromise systems, as noted in the Rules of Engagement.

## Appendix II: Comments from the U.S. Government Accountability Office

GAO U.S. GOVERNMENT ACCOUNTABILITY OFFICE

# Memorandum

**Date:** March 30, 2022

**To:** Inspector General, Nancy Birnbaum

**From:** CIO, Howard M. Williams, Jr. Howard M. Williams, Jr. Digitally signed by Howard M. Williams, Jr. Date: 2022.03.30 12:01:15 -04'00'
CAPO, Terrell G. Dorn Terrell G. Dorn, PE Digitally signed by Terrell G. Dorn, PE Date: 2022.03.30 09:21:23 -04'00'

**Subject:** Response to OIG 22-2, Information Security, dated March 15, 2022

GAO management agrees with the recommendations in OIG-22-2, *Information Security: Privacy Program Improvements Could Enhance GAO Efforts to Protect Data and Systems*, that GAO's privacy program could better define policies and procedures for assessing privacy impacts during incident response and for delivering training to individuals with access to PII. In coordination with the Privacy Office, Information Systems and Technology Services (ISTS) believes that GAO's current program generally aligns with NIST guidance, but we can take action to improve upon those aspects of our incident response and training identified in the OIG report. The report makes two recommendations with which GAO management concurs, as explained in further detail below.

The report recommends that GAO define and implement policies and procedures for incident response that align with NIST guidance for assessing privacy incident impacts (recommendation 1). Consistent with this recommendation, the Privacy Office will coordinate with ISTS and Security and Emergency Management (SEM) to update GAO Directive 0910-1-08, GAO Information Security Incident Response, to incorporate into existing processes additional policies and procedures for incident response more closely aligned with NIST guidance for assessing privacy incident impacts. This effort will include details for determining the impact of privacy data loss to external entities or persons, and will help ensure GAO responds effectively to privacy incidents. We expect to complete our update to the Directive by October 31, 2022.

The report also recommends that GAO define and implement policies and procedures for role-based privacy training that (a) identify who must regularly take the training, and (b) ensure annual compliance with such training (recommendation 2). Improvements to GAO's privacy training are already in the planning phases. The Privacy Office has outlined a plan for improving the privacy training to GAO staff, which will include the delivery of training to individuals with access to PII. The Privacy Office will be working with ISTS and the Learning Center to determine the best possible method for delivering annual and role-specific privacy training, and for ensuring compliance with such training requirements on an annual basis. We expect to complete and begin providing the updated Privacy Training to staff by October 31, 2022.

If there are any questions concerning this response, please contact the CIO.

cc: Karl Maschino, CAO
Paul Johnson, CAO
Jennifer Ashley, CAO
Chuck Gepford, ISTS
David Sadnavitch, ISTS
Lisa Binckes, IO
Adebiyi Adesina, FMBO
Mary Mohiyuddin, OIG

## Appendix III: OIG Contact and Staff Acknowledgments

### OIG Contact

L. Nancy Birnbaum, (202) 512-9355 or birnbauml@gao.gov.

### Staff Acknowledgments

In addition to the contact named above, Mary Arnold Mohiyuddin (Assistant Inspector General for Audit), Thomas J. Johnson (Engagement Manager), and Adriana Pukalski (Legal Counsel) made major contributions to this report. Other key contributors include Melanie H. P. Fallow and Cynthia Taylor.

## Appendix IV: Report Distribution

U.S. Government Accountability Office

Gene L. Dodaro – Comptroller General
Orice Williams Brown – Chief Operating Officer
Karl J. Maschino – Chief Administrative Officer/Chief Financial Officer
Edda Emmanuelli Perez – General Counsel
Howard M. Williams, Jr.– Chief Information Officer/Managing Directory Information Technology Systems and Services
Terrell G. Dorn – Managing Director Infrastructure Operations
Angela Nicole (Nikki) Clowers – Managing Director, Congressional Relations
Chuck Young – Managing Director, Public Affairs
William L. Anderson – Controller/Deputy Chief Financial Officer
Paul Johnson, Deputy Chief Administrative Officer
Adebiyi A. Adesina – Special Assistant to the Controller
Jennifer A. Ashley – Special Assistant for Operational Initiatives
Adrienne C. Walker – Director, Program Analysis and Operations

GAO Audit Advisory Committee

GAO Congressional Oversight Committees

## OIG Mission

Our mission is to protect GAO's integrity through audits, investigations, and other work focused on promoting the economy, efficiency, and effectiveness in GAO programs and operations, and to keep the Comptroller General and Congress informed of fraud and other serious problems relating to the administration of GAO programs and operations.

## Reporting Fraud, Waste, and Abuse in GAO's Internal Operations

To report fraud and other serious problems, abuses, and deficiencies relating to GAO programs and operations, you can do one of the following (anonymously, if you choose):

- Call toll-free (866) 680-7963 to speak with a hotline specialist, available 24 hours a day, 7 days a week.
- Visit https://gao-oig.listeningline.com/.

## Obtaining Copies of OIG Reports and Testimonies

To obtain copies of OIG reports and testimonies, go to GAO's website: https://www.gao.gov/ig or https://www.oversight.gov/reports, maintained by the Council of Inspectors General on Integrity and Efficiency.