GAO'S PRIVACY PROGRAM

Opportunities Exist to Further Protect Personally Identifiable Information (PII)

March 30, 2015

GAO'S PRIVACY PROGRAM

Opportunities Exist to Further Protect Personally Identifiable Information (PII)

Objective

The objective of our evaluation was to examine the extent to which GAO's privacy program protects PII under the authority and control of GAO.

What OIG Found

GAO has established a privacy program and is providing privacy awareness training to GAO staff and contractors. Our review identified opportunities to further protect PII from unauthorized access, use, or disclosure that could seriously harm individuals and the agency. For example, we identified GAO systems that unnecessarily collected Social Security Numbers and other systems that stored PII for periods beyond GAO's records retention schedule. Minimizing the collection and retention of PII are key practices for reducing privacy risks. We also identified a gap in GAO's background check procedures that resulted in access to confidential and sensitive PII by contractor personnel without background checks. Weak procedural safeguards do not mitigate the risk that the interests of a contractor may diverge from GAO's interests. In addition, we identified privacy documentation and notifications that were outdated or incomplete. Without documentation and notifications regarding PII, individuals may not be adequately informed regarding GAO's need to collect PII and its responsibility for protecting it. Finally, we determined that GAO's inventory of systems handling PII was incomplete, which diminishes GAO's ability to protect PII since it cannot protect what it doesn't know exists.

What OIG Recommends

OIG recommended that the Comptroller General (CG) direct the Chief Agency Privacy Officer to: minimize the use and retention of PII in GAO systems, notify individuals how and why their PII was collected and shared, identify and address gaps in privacy documentation for outsourced systems, and update the privacy office's inventory of systems handling PII. We also recommended that the CG direct the Chief Administrative Officer to update GAO security polices and procedures to require background checks for all contractors handling confidential or sensitive GAO data. GAO agreed with our recommendations and has taken or planned actions to address them.

March 30, 2015

Memorandum For: Gene L. Dodaro
Comptroller General of the United States

From: Adam R. Trzeciak
Inspector General

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

Attached for your information is our report, *GAO's Privacy Program: Opportunities Exist to Further Protect Personally Identifiable Information (PII)*. We provided GAO with a draft of this report for review and comment on March 4, 2015.

Our review found that GAO has established a privacy program based upon applicable laws and regulations and is providing privacy awareness training to GAO staff and contractors. However, we identify opportunities for enhancing privacy controls to better safeguard sensitive information and make seven recommendations aimed at improving GAO's privacy program. GAO agreed with our recommendations and has taken or planned actions to address them. 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 Audit Advisory Committee, and other key managers. This report is also available on GAO's website at http://www.gao.gov/about/workforce/ig.html.

If you have questions about this report, please contact me at (202) 512-5748 or trzeciaka@gao.gov.

Attachment

Table of Contents

Abbreviations

CAPO	Chief Agency Privacy Officer
CBPS	Competency Based Performance System
DM/ERMS	Document Management/Electronics Records Management System
e-QIP	Electronic Questionnaires for Investigations Processing
FAS	Financial Audit System
HCO	Human Capital Office
IESS	Integrated Electronic Security System
ISTS	Information Systems and Technology Services
MASS	Mainframe Audit Support System
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PPS	Payroll Personnel System
PTA	Privacy Threshold Analysis
SSN	Social Security Number
SORN	System of Records Notice
TRRS	Training Registration Resource System

Introduction

Privacy is an individual's ability to control the collection, use, and dissemination of his or her personally identifiable information (PII). PII refers to any information about an individual that (1) can be used to distinguish or trace the individual's identity, such as name, Social Security Number (SSN), date and place of birth, mother's maiden name, or biometric records; or (2) is linked or linkable to the individual, such as medical, educational, financial, and employment information.[1]

Federal agencies collect and use PII for a variety of reasons. Security breaches that result in unauthorized access, use, or disclosure of that PII can seriously harm individuals—leading to problems such as identity theft, blackmail, or embarrassment. These breaches also pose significant risks to agencies by reducing public trust or creating legal liabilities.

In response to increasingly sophisticated threats—including the exponential growth of information system hacking—and growing concerns regarding the availability of PII, citizens and legislators began to contemplate the ways that this information could be abused. This led to the establishment of privacy programs intended to define agency policies and practices, verify that their employees are following the practices and complying with policies, and confirm that third-party service providers are adequately protecting PII. Although GAO, as a legislative branch agency, is not subject to the privacy and information security laws applicable to executive branch agencies, GAO has established a privacy program based upon those laws. As individual demands and regulatory requirements change, agency privacy practices and policies must be reviewed and revised to meet this changing agency environment.

Objective, Scope, and Methodology

The objective of our evaluation was to examine the extent to which GAO's privacy program protects PII that is under GAO's authority and control. To achieve our objective, we selected and evaluated nine systems (six GAO and three outsourced) used to support GAO operations. These nine systems include:

---

[1]NIST, *Guide to Protecting the Confidentiality of PII*, NIST Special Publication 800-122 (Gaithersburg, Md.: April 2010).

GAO systems

1. Mainframe Audit Support System (MASS)
2. Integrated Electronic Security System (IESS)
3. Competency Based Performance System (CBPS)
4. Training Registration Resource System (TRRS)
5. WebTA
6. Financial Audit System (FAS)

Outsourced systems

7. Electronic Questionnaires for Investigations Processing (e-QIP)
8. HR Connect
9. Payroll Personnel System (PPS)

Our evaluation focused on compliance with applicable policies, procedures, laws, regulations; best practices from the National Institute of Standards and Technology (NIST)[2] and the Office of Management and Budget (OMB)[3]; and the following internal controls involved in GAO's privacy program:

- data minimization and retention: the volume of PII collected and stored, as well as the length of time data is maintained;

- authority and purpose: the legal authority and legitimate business need to collect, use, maintain, or share PII and providing notice to individuals regarding how their PII will be protected;

- accountability, audit, and risk management: broad areas related to privacy including assessing and mitigating risk at the agency level and the overall implementation and governance of the GAO privacy program; and

- security: establishing and updating an inventory of PII and maintaining an incident response plan in the event of a breach or unauthorized disclosure.

---

[2]NIST Special Publication 800-122 and NIST, *Security and Privacy Controls for Federal Information Systems and Organizations*, NIST Special Publication 800-53, revision 4 (Gaithersburg, Md.: April 2013).

[3]OMB, *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, M-03-22 (Washington, D.C.: September 26, 2003).

We also interviewed relevant GAO staff, including operational support managers and information technology personnel, to ensure our understanding of GAO's requirements and processes and to discuss issues found during our review. Additional information on our scope and methodology is presented in appendix I.

We conducted this evaluation from March 2014 to March 2015 in accordance with the quality standards established by the Council of Inspectors General on Integrity and Efficiency.[4] Those standards require that we plan and perform the evaluation to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our evaluation objectives.

Background

In the course of its daily operations and activities, GAO collects, uses, maintains, and shares PII in systems it owns as well as outsourced systems. The outsourced systems are used to support specific functions, such as payroll and travel transactions.

Executive branch agencies are subject to privacy requirements as set out in statutes, regulations, and guidance including the Privacy Act of 1974,[5] the Federal Information Security Management Act of 2002,[6] the E-Government Act of 2002,[7] and NIST and OMB guidance and best practices issued under those laws. Although GAO is not subject to these requirements, it is GAO policy[8] to protect personal privacy consistent with those laws. As such, GAO policy requires that:

- privacy interests of individuals are protected by imposing requirements of accuracy, relevance, and confidentiality for the maintenance and disclosure of personnel records; and

- notifications be made to inform individuals of

---

[4]CIGIE, *Quality Standards for Inspection and Evaluation*, (Washington, D.C.: January 2012).

[5]5 U.S.C. § 552a.

[6]44 U.S.C. § 3541, et seq.

[7]44 U.S.C. § 101.

[8]GAO Order 0450.1, *GAO Privacy Program* (April 5, 2013).

- o the existence of systems of records maintained by GAO containing personal records and information; and

- o their right to review and challenge the contents of personnel records containing their personal information.

GAO's Privacy Program

On April 5, 2013, GAO established its privacy program with the implementation of GAO Order 0450.1, *GAO Privacy Program*. GAO's privacy program, which is under the direction of the GAO Privacy Office, is intended to provide comprehensive and coordinated agency-wide protection for all PII under the authority or control of GAO. The GAO Privacy Office is directed by the Chief Agency Privacy Officer (CAPO) and includes a Records Officer, management analyst, and an advisor from the GAO Office of General Counsel. The mission of the Privacy Office is to preserve and enhance privacy protections for PII and to promote transparency of GAO privacy operations. General requirements outlined in GAO's privacy policy include policies and procedures to:

1. identify holdings of PII under the authority or control of GAO;
2. periodically assess the risks of harm to the privacy of individuals through the misuse of PII under the authority or control of GAO, including through the conduct of privacy impact assessments (PIA) [9] of significant new or changing uses of PII in information systems;
3. develop and maintain controls for the generation, collection, processing, maintenance, storage, dissemination, recovery, and disposal of PII to protect privacy by cost-effectively reducing privacy risks to an acceptable level;
4. ensure the efficient and effective implementation of privacy procedures for personnel records;[10]
5. detect and respond to privacy incidents, including undertaking remedial action to address deficiencies in the use or protection of PII;

---

[9]A PIA is an analysis of how PII is collected, used, shared, maintained, and disposed of for a specific information system. The purpose of a PIA is to identify potential privacy risks and develop plans to mitigate those risks.
[10]The agency's privacy procedures for personnel records are codified at 4 C.F.R. Part 83.

6. periodically test and evaluate the effectiveness of GAO privacy policies, procedures, and practices; and

7. provide initial and annual refresher training to all covered persons[11] to ensure that they understand the privacy risks associated with their activities and understand their responsibilities for complying with GAO privacy policies and procedures to reduce these risks.

Following establishment of its Privacy Office, GAO conducted privacy threshold analyses (PTA)[12] and PIAs to determine whether GAO systems had privacy implications and if so, identified how PII is collected, maintained, stored, and disposed. In response to a prior OIG evaluation,[13] in March 2014, GAO provided privacy training to the following GAO offices: Financial Management and Business Operations, Human Capital Office (HCO), and Information Systems and Technology Services (ISTS). GAO also extended privacy awareness training to all GAO employees and contractors as part of its 2014 Mandatory eLearning Training Curriculum. Further, the GAO Privacy Office participated in GAO's National Preparedness Month Fair, by distributing to GAO staff materials describing GAO's Privacy Program and actions individual staff could take to protect their privacy.

Opportunities Exist to Further Protect PII

Our review of six internal GAO systems and three systems that support outsourced GAO functions, identified opportunities to strengthen GAO's privacy program and the protection it provides over PII. Specifically, we found that additional actions were needed to reduce the potential risk of PII misuse by limiting the use of PII as an identifier and enforcing existing retention policies. In addition, we identified a security risk due to a procedural gap that permitted GAO contractors access to PII without a background check.

Internal GAO Systems Unnecessarily Collect and Store PII

GAO systems generally collect and store PII to uniquely identify individuals when creating or retrieving data specific to an individual or linking that data to another data file or information

---

[11]A covered person, for the purpose of mandatory privacy training, refers to all GAO employees and contractors.

[12]A PTA is used to document determinations regarding whether an information system has privacy implications that require a PIA.

[13]OIG, *Information Security: Evaluation of GAO's Information Security Program and Practices for Fiscal Year 2009*, OIG-10-3 (Washington, D.C.: January 4, 2010).

system. Best practices show that an agency can reduce their privacy and security risk by minimizing the collection of PII and reducing their inventory of PII.[14] These data minimization controls include:

- limiting the collection and retention of PII to the minimum elements that are relevant and necessary to accomplish the legally authorized purpose;
- regularly reviewing the PII collected and retained to ensure that it continues to be necessary to accomplish the legally authorized purpose; and
- disposing of, destroying, erasing, or anonymizing PII in accordance with an approved retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access.

One best practice for minimizing the exposure of PII is using a unique identifier, such as a generic employee number, to identify individuals within an organization. The use of SSNs for internal training and performance systems has long been identified as unnecessary and a privacy risk due to the potential for identity theft if a system were compromised. We found that two[15] of the six GAO systems reviewed use SSNs rather than employee numbers to identify individuals. Interviews with appropriate GAO records management and information technology managers for the two systems using SSNs confirmed that their systems do not need to use SSNs as identifiers. Minimizing the use of SSNs would reduce the risk that SSN data would be inadvertently shared or disclosed.

The GAO Records Officer acknowledged the need to phase out SSN usage in GAO systems and stated that ISTS is developing plans to address this issue. According to internal e-mail messages from June 2012 and interviews with relevant personnel, GAO has not focused attention on unique identifiers because of resource constraints and the possibility of moving to new outsourced systems that do not rely on SSNs. However, the planned migration to outsourced training and performance systems has been delayed. During an October 21, 2014 briefing to the GAO Information Technology Investment Committee, GAO staff estimated that the Treasury Learning/Performance Management System, which GAO was considering to replace its legacy system, could not be

---

[14]NIST Special Publication 800-53, revision 4.
[15]CBPS and TRRS.

implemented before the first quarter of fiscal year 2017. According to GAO, Treasury has temporarily prevented additional agencies from moving to the Treasury Learning/Performance Management System while it works with a third-party vendor to add functionality to the system. Given this new information, GAO management must weigh the risk of continuing to use SSNs for internal training and performance systems against the cost of updating existing GAO systems.

Disposing of, destroying, erasing, or anonymizing PII in accordance with an approved retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access is a key data minimization control for safeguarding PII. However, we found that of the nine systems reviewed, seven[16] maintained PII for periods beyond GAO's records retention schedule.[17] According to GAO's records retention schedule and the GAO System of Records Notice (SORN), time and attendance records, as well as individual employee payroll records, are to be destroyed 7 years after the end of the fiscal year in which they are created. Still, we found that WebTA—which collects employee names, SSNs, and other sensitive data—maintained time and attendance data back to 2003, a period of over 11 years. According to GAO staff responsible for the systems reviewed, efforts are under way to either archive or delete data in order to conform to record retention policies and procedures. The GAO Records Officer added that the disposal of records in business systems outside of GAO's Document Management/Electronic Records Management System (DM/ERMS) system[18] was part of the 2014 *Records and Privacy Work Plan*.

Background Checks Were Not Performed for all Contractors Handling GAO PII

Federal entities typically perform background checks to provide some assurance that an individual is trustworthy and not likely to cause harm to the organization. Although not as rigorous as the security clearance process, background checks support accountability, audit, and risk management by potentially identifying questionable activity in an individual's past

---

[16]MASS, CBPS, TRRS, WebTA, e-QIP, HR Connect, and PPS.

[17]GAO *Records Information and Disposition Schedules* (October 1, 2007).

[18]DM/ERMS is GAO's official records management system used to: capture and preserve documents/records that are important evidence of how GAO conducts business, protect the integrity of the documents and the files, and provide ready access to record materials required to support GAO's engagements and business activities and processes.

OIG-15-1 GAO Privacy Program

before granting the individual access to sensitive information. NIST and GAO recommend background checks for external third parties, such as contractors.[19]

We identified a gap in GAO's background check procedures that resulted in access to GAO PII by contractor personnel without background checks. Specifically, GAO's security policy and related directive on contractors[20] do not require background checks for contractors, including those with access to GAO PII unless physical access to a GAO facility is required or a GAO office requests the background check. As a result, background checks were not conducted for contractors performing actuarial services to estimate GAO's workers compensation and retirement liabilities, which involved GAO PII.

Absent background checks, GAO appeared to rely on signed non-disclosure agreements to protect against unauthorized disclosure of sensitive information. GAO's reliance on non-disclosure agreements to ensure the safety of its sensitive data does not mitigate the risk that the interests of a contractor or its staff may diverge from GAO's interests. Weak procedural safeguards increase GAO's risk that contractor personnel who have questionable backgrounds may inappropriately obtain and use GAO PII.

Opportunities Exist to Improve PII Notifications

Agencies use authority and purpose controls to identify the legal authority for collecting PII or for engaging in other activities that affect privacy, and to describe the purpose of PII collection in privacy notices, such as system log-in pages and warning banners, and SORNs. Our review found that GAO has taken steps to improve its PII notifications, including

- updating system log-in pages and warning banners to notify users of system and data restrictions, including PII, publishing SORNs in the *Federal Register*[21] to

---

[19] NIST Special Publication 800-53, revision 4 and GAO, *Federal Information System Controls Audit Manual (FISCAM)*, GAO-09-232G (Washington, D.C.: February 2009).

[20] GAO Order 0910.1, *GAO Security Program* (July 1, 2013); and GAO Directive 0910.1-05, *Industrial Security Program Requirements for GAO Contractors* (July 1, 2013).

[21] For federal agencies, the need to collect PII, including the collection or grouping of retrievable information by some identifier unique to an individual, should also be publicly announced as a SORN in the *Federal Register*,

communicate the agency's need for collecting not only a specific item of personal information, but also the collection or grouping of information about an individual that can be retrieved by the name of the individual or by some other type of unique identifier for the individual, and

- conducting PIAs, which also provide notice to the public of privacy practices and help to ensure that projects, programs or information systems comply with legal, regulatory, and policy requirements and should be updated when changes create new privacy risks.

Notices of new information collections and details regarding how personal information will be used and protected are central to providing individuals with privacy protections and transparency. While GAO's actions help communicate what personal information is collected, how it's maintained, and with whom the information is shared, we identified areas where improvements could be made to help ensure that systems containing PII are identified and individuals are notified of GAO's need to collect personal information and its responsibility for protecting it.

Of the six GAO systems reviewed, four[22] systems lacked a privacy notice on the system's log-in page or as part of its warning banner. According to NIST guidance,[23] an agency should describe the purpose(s) for which PII is collected, used, maintained, and shared in its privacy notices. During our review, GAO developed and posted a privacy notice on a module for one[24] of the four systems we found lacking privacy notices. The GAO Records Officer stated that posting privacy notices for the remaining system modules is an action item for the privacy team. Without notification regarding PII, users may not be adequately informed regarding how or why their personal information was collected and with whom it was shared.

---

which is compiled by the Office of the Federal Register (within the National Archives and Records Administration) and is printed by the Government Printing Office.

[22]IESS, CBPS, TRRS, and WebTA.

[23]NIST Special Publication 800-53, revision 4.

[24]The privacy notice was posted on the IESS Visitor Management module.

In addition to on-line notifications and banners, agencies use SORNs to communicate their need to collect not only a specific item of personal information, but also the collection or grouping of information about an individual that is retrievable by the individual's name or by some other type of unique identifier for the individual. Of the six GAO systems reviewed, two[25] were not included in a SORN published in the *Federal Register*. As a result, GAO may be collecting and sharing PII without a clear or approved need, thereby increasing the risk of misuse and unauthorized disclosure.

GAO guidance and NIST best practices[26] require that PIAs be conducted to identify privacy risks and methods to mitigate those risks when developing, procuring, or making a significant change to an information system that collects, uses, maintains, or shares PII. PIAs provide notice to the public of privacy practices, and help to ensure that projects, programs or information systems comply with legal, regulatory, and policy requirements. As such, they should be updated when changes create new privacy risks. However, our review of nine GAO and outsourced systems found that eight PIAs were outdated. For example, we found that PIAs for five[27] of the six GAO systems reviewed did not specify whether a system of records was created under the Privacy Act of 1974.[28] Regarding the three outsourced systems reviewed, we found that PIAs for:

- two systems did not specify any agreements that govern the disclosure of PII and its use by non-GAO persons/organizations,[29]
- two systems did not explain how privacy, records management, and security of GAO data were addressed,[30] and
- two systems did not specify the extent to which individuals have the right to consent to the use of their PII.[31]

According to GAO and OMB guidance, [32] a PIA shall consist of a description and analysis of:

---

[25]IESS and TRRS.

[26]GAO Order 0450.1 and NIST Special Publication 800-53, revision 4.

[27]MASS, IESS, CBPS, TRRS, and WebTA.

[28]74 Fed. Reg. 40818 (Aug. 13, 2009).

[29]e-QIP and PPS.

[30]e-QIP and PPS.

[31]HR Connect and PPS.

[32]GAO Order 0450.1 and OMB M-03-22.

- the use (e.g., any collection, creation, maintenance, processing, storage, transmission, or dissemination) of PII by an information system;
- the privacy risks created by the use of PII by the system; and
- actions taken to address and mitigate such privacy risks, including the consideration of alternative approaches to reduce such risks, and the controls to be used to reduce such risks.

To ensure the completeness of its assessment of privacy risk and documentation of methods used to mitigate any identified risks, GAO policy requires the use of a template, available on the GAO intranet, to develop a PIA for any system collecting or storing PII. System owners are required to submit their draft PIAs to the Privacy Office for review and approval by the CAPO. These requirements also extend to changes or updates to existing systems that may have an impact on privacy. Finally, PIAs are to be updated every three years for existing systems regardless of changes or updates. While GAO's Privacy Program guidance and template(s) help strengthen compliance with policies and procedures for collecting and storing PII for newer systems, GAO's Privacy Office has not initiated an effort to update older PIAs to help ensure compliance with the updated policy and requirements that may have emerged since the initial PIA was approved. PIAs for six[33] of the nine GAO and outsourced systems reviewed were prepared prior to the development and posting of the new template.

Enhancements are Needed to Improve Oversight and Monitoring of PII

NIST guidance states that "an organization cannot properly protect PII it does not know about" and "organizations should identify all PII residing in their environment."[34] Protecting privacy is best achieved when security, and accountability, audit, and risk management controls are an integral part of agency operations. Processes and procedures for identifying and tracking PII, including maintaining a PII inventory, enables agencies to implement effective administrative, technical, and physical security policies and procedures to protect PII and mitigate risks of PII exposure.

---

[33]e-QIP, FAS, HR Connect, PPS, TRRS, and WebTA.

[34]NIST Special Publication 800-122.

Though GAO has taken some important steps to identify its collection, use, and sharing of PII, including the use of PIAs to identify and manage privacy risk and the establishment of an inventory of PII-related systems, we found that GAO's PIAs for eight systems reviewed were outdated. We also found that the CAPO lacked a process to identify and track PII collected or used throughout the agency, including PII shared with other agencies through outsourced systems. For example, we found that GAO engagement teams[35] may enter into a Memorandum of Agreement with other agencies involving the sharing of PII without notifying the CAPO. Further, PIAs for outsourced systems may not be developed or reviewed by the Privacy Office to ensure that they contain all of the elements in the GAO Privacy Program and templates. NIST guidance describes how an agency can monitor and audit privacy controls and internal privacy policy to ensure effective implementation. Specifically, agencies should conduct regular assessments (e.g., internal risk assessments) to promote accountability, and identify and address gaps in privacy compliance, management, operational, and technical controls. These assessments can be self-assessments or third-party audits that result in reports on compliance gaps identified in programs, projects, and information systems.[36] The lack of visibility and monitoring by the CAPO of PII shared with other agencies increases the risk of unauthorized access to GAO PII and diminishes assurances that appropriate technical, procedural, and operational safeguards are in place consistent with GAO requirements.

We also found that although the CAPO had established an inventory of systems collecting, using, maintaining, or sharing PII to use in fulfilling its mission of protecting PII, the CAPO's inventory was incomplete. Specifically, we found that the systems inventory used by the CAPO did not include 38 systems that the HCO identified as collecting, using, maintaining, or sharing PII. Further, the CAPO did not conduct an internal risk assessment of systems included in its inventory to identify and address gaps in privacy compliance. As a result, GAO may not have fully identified the extent to which it captures and uses PII and taken

---

[35]The GAO workforce is organized largely by subject area, with most employees being in one of the following 14 teams: Acquisition and Sourcing Management; Applied Research and Methods; Defense Capabilities and Management; Education, Workforce, and Income Security; Financial Management and Assurance; Financial Markets and Community Investment; Forensic Audits and Investigative Service; Health Care; Homeland Security and Justice; Information Technology; International Affairs and Trade; Natural Resources and Environment; Physical Infrastructure; and Strategic Issues.

[36]NIST Special Publication 800-53, revision 4.

appropriate steps to ensure that the data are adequately safeguarded and the risk of misuse or unauthorized disclosure is mitigated.

NIST guidance describes how an agency can establish, maintain, and update an inventory that contains a listing of all programs and information systems identified as collecting, using, maintaining, or sharing PII.[37] One suggested method of gathering information for a PII inventory is to extract information from PIAs for systems containing PII, including the:

- name and acronym for each system identified;
- types of PII contained in that system;
- sensitivity of all types of PII; and
- potential risk of substantial harm, embarrassment, inconvenience, or unfairness to affected individuals, as well as the financial or reputational risks to organizations, if PII is exposed.

However, resource constraints may have contributed to the CAPO's ability to establish and maintain an inventory to monitor and oversee the agency's collection and use of PII. At the start of our review, GAO's privacy policy had been final for less than a year and there were less than two full-time staff available to assist the CAPO in executing the program. According to an April 2014 workforce plan, GAO planned to hire two additional staff for its privacy office. GAO filled one of the two positions in fiscal year 2014. According to the GAO Records Officer, additional staff will provide the resources needed to ensure that PIAs and other privacy documentation are reviewed and updated timely.

Recommendations

We are making seven recommendations aimed at enhancing GAO's privacy program and efforts to safeguard sensitive information in GAO and outsourced systems. Specifically, we recommend that the Comptroller General direct the CAPO to take the following six actions:

1. Coordinate with system owners to develop and implement a set of unique employee identifiers that are not SSNs for use in internal GAO systems.

---

[37]NIST Special Publication 800-53, revision 4.

2. Coordinate with system owners to ensure that record retention policies and PIA documents are accurate/valid and followed (i.e., PII data are archived or deleted based on business requirements).

3. Develop and post comprehensive privacy notices for IESS, CBPS, TRRS, and WebTA.

4. Review PIAs provided by vendors/agencies of outsourced systems for each item required in the current GAO PIA template and develop a plan to obtain additional information or assurance(s) for any gaps identified.

5. Validate the privacy office's inventory of systems identified as collecting, using, maintaining, or sharing PII and meet with representatives from each GAO team to ensure the list is complete.

6. Conduct an internal risk assessment of GAO systems to identify and address gaps in privacy compliance from best practices, such as NIST Special Publication 800-53, revision 4 and NIST Special Publication 800-122.

In addition, we recommend that the Comptroller General direct the Chief Administrative Officer to:

7. Update GAO Order 0910.1, *GAO Security Program*, and GAO Directive 0910.1-05, *Industrial Security Program Requirements for GAO Contractors*, to require the Office of Security and Emergency Management to perform background checks for all contractors handling GAO PII or obtain similar assurance, such as using cleared contractors.

Agency Comments and Our Evaluation

The Inspector General provided GAO with a draft of this report for review and comment. GAO provided written comments, which are reprinted in appendix II. GAO agreed with our recommendations and described actions taken or planned to mitigate the control risks identified in our work. The agency also provided technical comments that we incorporated, as appropriate.

Actions taken in response to our recommendations are expected to be reported to our office within 60 days.

Appendix I: Objective, Scope, and Methodology

The objective of our evaluation was to examine the extent to which GAO's privacy program protects personally identifiable information (PII) that is under GAO's authority and control. To achieve our audit objective, we selected and evaluated nine systems (six GAO and three outsourced) used to support GAO operations. These nine systems include:

GAO systems

1. Mainframe Audit Support System (MASS)
2. Integrated Electronic Security System (IESS)
3. Competency Based Performance System (CBPS)
4. Training Registration Resource System (TRRS)
5. WebTA
6. Financial Audit System (FAS)

Outsourced systems

7. Electronic Questionnaires for Investigations Processing (e-QIP)
8. HR Connect
9. Payroll Personnel System (PPS)

We reviewed applicable policies, procedures, laws, and regulations, including GAO Orders 0410.1, *The GAO Records Management Program*,[38] 0450.1, *GAO Privacy Program,*[39] and 0910.1, *GAO Security Program*;[40] the Privacy Act of 1974;[41] Federal Information Security Management Act of 2002;[42] E-Government Act of 2002;[43] and best practices contained in the National Institute of Standards and Technology (NIST) guidance[44] to identify key security and privacy information system control principles as criteria for evaluating GAO's privacy program. Based on that review, we focused our evaluation of the nine systems on four key control principles of GAO's privacy program. These specific control principles included: (1)

---

[38]GAO Order 0410.1, *The GAO Records Management Program* (March 2, 2004).

[39]GAO Order 0450.1, *GAO Privacy Program* (April 5, 2013).

[40]GAO Order 0910.1, *GAO Security Program* (July 1, 2013).

[41]5 U.S.C. § 552a.

[42]44 U.S.C. § 3541, et seq.

[43]44 U.S.C. § 101.

[44]NIST, *Guide to Protecting the Confidentiality of PII*, NIST Special Publication 800-122 (Gaithersburg, Md.: April 2010) and NIST, *Security and Privacy Controls for Federal Information Systems and Organizations*, NIST Special Publication 800-53, revision 4 (Gaithersburg, Md.: April 2013).

data minimization and retention; (2) authority and purpose; (3) accountability, audit, and risk management; and (4) security. Data minimization and retention evaluated the volume of PII collected and stored, as well as the length of time data is maintained. Authority and purpose referred to the legal authority and legitimate business need to collect, use, maintain, or share PII. It also included providing notice to individuals regarding how their PII will be protected. Accountability, audit, and risk management covered broad areas related to privacy including assessing and mitigating risk at the agency level and the overall implementation and governance of the GAO privacy program. Finally, security controls included establishing and updating an inventory of PII and maintaining an incident response plan in the event of a breach or unauthorized disclosure.

To supplement our understanding of GAO's privacy program and controls, we interviewed the GAO Records Officer who administers GAO's privacy program and managers from business units, such as the Human Capital Office and Infrastructure Operations that obtain and use PII on a regular basis. In addition, we interviewed system owners and technical representatives and reviewed the applicable privacy documentation, including: privacy impact assessments, privacy notices, and the GAO Human Capital Management System of Record Notice published in the *Federal Register*.

We conducted this evaluation from March 2014 to March 2015 in accordance with the quality standards established by the Council of Inspectors General on Integrity and Efficiency.[45] Those standards require that we plan and perform the evaluation to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our evaluation objectives.

---

[45]CIGIE, *Quality Standards for Inspection and Evaluation*, (Washington, D.C.: January 2012).

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

GAO U.S. GOVERNMENT ACCOUNTABILITY OFFICE

Memorandum

Date: March 24, 2015

To: Inspector General – Adam Trzeciak

From: Managing Director, Infrastructure Operations – Terrell Dorn

Subject: Draft Report on GAO's Privacy Program (OIG-15-1)

Thank you for the opportunity to review and comment on your draft report on GAO's Privacy Program. I appreciate the professionalism and courtesy with which you and your staff conducted this audit. As noted in your report, GAO has a comprehensive privacy program in place to protect the data we collect. We also recognize the importance of maintaining the security of the privacy data in our systems and continuously look to make improvements to the privacy program. We appreciate the recommendations in your report and believe that they align with the improvements we already have planned or are underway. I have outlined below our planned actions in these areas and the current timeline for implementation.

Recommendation 1: Coordinate with system owners to develop and implement a set of unique identifiers that are not SSNs for use in internal systems.

Response: GAO's Privacy Office will coordinate with appropriate stakeholders to limit the use of social security numbers in IT systems, as deemed necessary to comply with GAO's records policy. (*Planned Completion Date: December 31, 2015*)

Recommendation 2: Coordinate with system owners to ensure that record retention policies and PIA documents are accurate, valid and followed.

Response: The Privacy Team folded the disposition of business records held outside of DM into its 2014 records management work plan, and it is addressed annually in the Records and Privacy strategic initiatives each year as an ongoing action item. Systems that we have added to our 2015 strategic initiatives are: MASS, IESS, CBPS, TRRS, WebTA, e-QIP (3rd party), HR Connect, and PPS (i.e. NFC). Financial Audit System records are exported automatically from that system into DM, and the data is controlled by the automated disposition routines in DM. In addition, we recently put 2009 and 2010 PIAs on their review cycle this year to re-evaluate their PII content, system functionality, and the system controls. This action item is on our current Records and Privacy strategic initiatives for 2015. (*Planned Completion Date: September 30, 2015*)

Recommendation 3: Develop and post privacy notices for IESS, CBPS, TRRS, and WebTA.

Response: A privacy notice has been developed and posted for IESS. The WebTA notice is in the process of being posted by HCO. Notices for CBPS and TRRS are in the Records and Privacy 2015 strategic initiatives. (*Planned Completion Date: September 30, 2015*)

Recommendation 4: Review PIAs provided by vendors/agencies of outsourced systems for each additional item required in the current GAO PIA template and develop a plan to obtain additional assurances for any gaps identified.

Response: Response: GAO's Privacy Office will collaborate with AM and OGC to develop privacy requirements, and procedures for reviewing PIAs, to ensure they meet GAO's privacy requirements for third-party agreements and contracts. *(Planned Completion Date: September 30, 2015)*

Recommendation 5: Validate the privacy office's inventory of systems identified as collecting, using, sharing PII and meet with representatives of each team to ensure the list is complete.

Response: ISTS will execute a strategic approach to identify and maintain an authoritative inventory of PII data/information usage within official GAO systems. ISTS will provide and report this information to GAO's Privacy Office on an as needed and periodic delivery basis. *(Planned Completion Date: September 30, 2015)*

Recommendation 6: Conduct an internal risk assessment of GAO systems to identify and address gaps in privacy compliance such as NIST SP 800-53 and NIST SP 800-122.

Response: The Privacy Team has this action item on its 2015 list of strategic initiatives using NIST SP 800-53, Appendix J and 800-122 as its guide. *(Planned Completion Date: September 30, 2015)*

Recommendation 7: Update Order 0910.1 – *GAO Security Program* and GAO Directive 0910.1-05, *Industrial Security Program Requirements for GAO Contractors* to require the Office of Security and Emergency Management to perform background checks for all contracts handling confidential or sensitive GAO data or obtain similar assurance, such as using cleared contractors.

Response: The Office of Security and Emergency Management has updated the language in GAO Order 0910.1 and GAO Directive 0910.1-05 to reflect the new policy. Both the order and directive are currently being reviewed by OGC and LMR. However, the Office of Security and Emergency Management has already implemented and currently performs background checks for all contractors handling confidential or sensitive GAO data. *(Planned Completion Date: September 30, 2015)*

I look forward to updating you on our progress as we continue to implement improvements to GAO's Privacy Program. Please contact me if you have any questions.

cc: Karl Maschino, Chief Administrative and Financial Officer
William Anderson, Controller
Nancy Hunn, Director, GAO Records Officer, IO

Page 2

Appendix III: Major Contributors to This Report

Douglas Carney was the engagement manager for this review. Other key contributors included Evelyn Logue and Cynthia Hogue.

Appendix IV: Report Distribution

<u>U.S. Government Accountability Office</u>

Patricia A. Dalton – Chief Operating Officer
Karl J. Maschino – Chief Administrative Officer/Chief Financial Officer
Susan A. Poling – General Counsel
William L. Anderson – Controller/Deputy Chief Financial Officer
Terrell G. Dorn – Chief Agency Privacy Officer
Nancy O. Hunn – GAO Records Officer
Carolyn M. Taylor – Chief Human Capital Officer
Howard M. Williams Jr. – Chief Information Officer
Adebiyi Adesina – Special Assistant to the Controller

<u>GAO Audit Advisory Committee</u>

OIG

Office of Inspector General
U.S. Government Accountability Office