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

INSPECTION REPORT

NUMBER 22-07

GPO's Privacy Program Inspection

July 29, 2022

Questions, Copies, Suggestions

The Inspections Division, Office of the Inspector General, GPO, prepared this report. If you have questions about the report or want to obtain additional copies, contact the Office of the Inspector General, GPO.

To suggest ideas for or request future inspections of GPO issues, contact the Office of the Inspector General, GPO:

Telephone: 1-800-743-7574

Fax: 202-512-1352

e-mail: gpoighotline@gpo.gov

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

U.S. GOVERNMENT PUBLISHING OFFICE

OIG

OFFICE *of the* INSPECTOR GENERAL

Report violations of law, rules, or agency regulations, mismanagement, gross waste of funds, abuse of authority, danger to public health and safety related to the U.S. Government Publishing Office contracts, programs and/or employees.

All reports are made in strict confidence

Hotline 1-800-743-7574

Email: gpoighotline@gpo.gov

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

MEMORANDUM
OIG-22-016

Date

July 29, 2022

To

Director, U.S. Government Publishing Office

From

Inspector General

Subject:

Final Report— GPO's Privacy Program Inspection, Report Number 22-07

Enclosed is the subject final report. The Office of the Inspector General (OIG) conducted an inspection of the GPO Privacy Program. We reported 4 findings and made 13 recommendations to improve GPO's Privacy Program. The recommendations focus on compliance and recordkeeping, incident response plans and guidelines, and training.

GPO reviewed the draft report and provided comments through the Director. In accordance with the Council of the Inspectors General on Integrity and Efficiency standards for inspections, we reviewed GPO's comments for relevance and completeness and included them in appendix D. We redacted the name of a specific OIG employee, as it is our practice not to publish employee names. Otherwise, GPO's comments are included in their entirety. We made changes to the report where relevant and informed by the management comments.

GPO concurred with all 13 recommendations and the proposed actions were generally responsive to the recommendations. We summarize management's comments and provide a detailed response throughout the body of the report. All recommendations remain open at this time.

If you have any questions or comments about this report, please contact Ashley Kehoe, Office Manager, at akehoe@gpo.gov.

Digitally signed by Michael P. Leary
Date: 2022.07.29 13:52:21 -04'00'

MICHAEL P. LEARY
Inspector General

Report No. 22-07 **July 29, 2022**

RESULTS IN BRIEF

What We Did

The Office of the Inspector General (OIG), Inspections Division, reviewed the effectiveness and efficiency of the U.S. Government Publishing Office's (GPO) Privacy Program and its management of personally identifiable information (PII). Specifically, the objectives were to: (1) determine if GPO policies governing the Privacy Program are aligned to Federal laws, regulations, guidance, and best practices, (2) quantify to what extent GPO collects, uses, stores, retains, and disposes of PII, (3) evaluate GPO's response to privacy breaches that occurred in the past 3 years (2018 - 2020), and (4) evaluate the overall effectiveness and efficiency of GPO's Privacy Program implementation.

What We Found

Finding 1. GPO states that its Privacy Program is aligned with Federal law and oversight guidance, specifically from the Privacy Act, the Office of Management and Budget (OMB), and the National Institute of Standards and Technology (NIST). However, GPO omits the inclusion of Systems of Records Notices, a basic privacy practice from the Privacy Act. GPO also lacks transparency in what privacy laws and guidance it follows and why. According to GPO's privacy website, GPO places a high priority on protecting PII and has aligned its Privacy Program directive to federal law and oversight guidance as best practices.[1] While as a Legislative branch agency, GPO is not required to follow federal laws designed to govern the Executive branch, GPO generally adheres to U.S. privacy governance, including OMB and NIST guidance. However, GPO does not specifically detail what federal laws and guidance they do follow in all cases nor the bases for their deviations from federal best practices. Of particular concern is GPO's omission of the Privacy Act's System of Records Notice (SORN) requirement, an otherwise standard privacy practice within the federal government.[2] Therefore, GPO's Privacy Program falls short of a thorough privacy program where PII is protected during all stages of the information life cycle, creating the possibility of PII loss, compromise, or unauthorized disclosure.

Finding 2. GPO needs to improve recordkeeping and PII management compliance for the 24 PII systems identified. During our review, we found that the Privacy Officer was aware of 19 GPO PII systems that collect, use, store, and retain PII; but was unaware of five

[1] https://www.gpo.gov/privacy

[2] *The Privacy Act of 1974*, as amended, 5 United States Code (U.S.C.) Section 552a, defines a system of record as a group of any records under the control of an agency that retrieves information by some identifying characteristic, such as an individual's name or some identifying number. Agencies that maintain systems of records are to publish notices of the existence and character of the system of records, including the routine use of the records in the system and policies regarding storage, retrievability, retention, and disposal of the records.

additional PII systems used by the Business Units (BUs). GPO was unable to produce PII confidentiality impact levels for these systems, and had not created compliance documents for all PII systems.[3] Since 2017, GPO has not conducted any Privacy Compliance Reviews (PCRs) for the systems that collect, use, and store PII. Further, GPO's directive governing retention and disposal of records does not include guidance on the identification of records containing PII. Without identifying the confidentiality impact level, maintaining compliance documents, and conducting PCRs, GPO risks failing to design and implement appropriate safeguards to protect PII, and the systems that contain PII, from unauthorized access or disclosure.

Finding 3. GPO's privacy incident response procedures should incorporate NIST Special Publication 800-122 in order to provide more detailed implementation guidance when responding to privacy incidents and breaches. GPO's Privacy Program includes a process to identify, report, investigate, and respond to privacy incidents. However, GPO's PII Incident Response Plans do not include NIST Special Publication 800- 122 guidance, omitting essential steps in implementing incident response, such as instructions on how to notify appropriate individuals and organizations. Without thorough Incident Response Plans, GPO risks failing to adequately evaluate and respond to suspected PII breaches.

Finding 4: GPO should ensure that all employees receive PII training. Over the period of this report, GPO did not provide privacy awareness training to all employees and contractors. GPO's Privacy Program directive requires each BU to ensure that individuals who could access, use, or disclose PII on GPO information systems receive appropriate training before being granted access. Additionally, the Privacy Officer is required to maintain the training program for employees having access to or managing PII. Any employee, regardless of their occupation, could be exposed to PII. Therefore, we assess, and benchmarking supports, that all employees should receive PII training. Further, we recommend that PII training be centralized under a single BU, likely Information Technology, to ensure employees and contractors receive PII training before accessing GPO's information systems.

What We Recommend

Our report contains 13 recommendations designed to improve the effectiveness of GPO's Privacy Program. The recommendations focus on compliance and recordkeeping, incident response plans and guidelines, and training.

[3] Confidentiality impact levels of low, moderate, or high indicate the potential harm that could result from inappropriately accessed, used, or disclosed PII. PII confidentiality impact levels determine the appropriate safeguards that can be applied to the PII.

CONTENTS

INTRODUCTION

The inspection team reviewed the effectiveness and efficiency of GPO's Privacy Program and PII management, to include the creation, protection, and destruction of PII. Based on our findings, we made 13 recommendations (appendix A). The scope and methodology are presented in appendix B.

Background

The GPO OIG initiated this review from its fiscal year 2021 annual work plan. Prior to the conclusion of fieldwork, GPO updated its Privacy Program directive, and we considered that directive in our review and analysis.[4] We acknowledge the possibility of program improvements and enhancements since fieldwork, and in support of the GPO Director's February 2022 response at a hearing before the Committee on House Administration that the agency constantly reviews and assesses the Privacy Program's associated policies and practices.[5]

It is GPO's stated policy to protect the access to and confidentiality of PII and Protected Health Information (PHI), which GPO collectively refers to as PII.[6] PII protection is especially important when information is sensitive in nature as with Social Security Numbers (SSN), legal proceedings, and medical information. PII is information that "can be used to distinguish or trace an individual's identity, such as their name, [SSN], or biometric records… alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth," or mother's maiden name.[7] GPO's Privacy Program aims to protect PII from the loss, compromise, or unauthorized disclosure that may potentially lead to identity theft or other fraudulent use resulting in substantial harm, embarrassment, inconvenience, or unfairness to the affected individuals and tarnish the agency's reputation.

The Issue

The U.S. government experienced several high-profile data breaches in recent years. For example, in 2015, the Office of Personnel Management (OPM), the agency that serves as the chief human resources agency and personnel policy manager for the Federal government, announced two separate, but related cybersecurity incidents that impacted the PII data of millions of Federal government employees, contractors, and others, as described below.

---

[4] GPO Directive 825.41B, Privacy Program: Protection of Personally Identifiable Information (PII), April 06, 2021.
[5] "Big Data: Privacy Risks and Needed Reforms in the Public and Private Sectors" Testimony before the Committee on House Administration, February 16, 2022.
[6] GPO Directive 825.41B, Privacy Program: Protection of Personally Identifiable Information (PII), April 06, 2021, p. 1.
[7] Ibid, p. 2.

In June 2015, OPM discovered that the background investigation records of current, former, and prospective federal employees and contractors had been stolen. OPM and the interagency incident response team concluded that sensitive information, including the SSNs of 21.5 million individuals, was stolen from the background investigation databases. This included 19.7 million individuals that applied for a background investigation, and 1.8 million non-applicants, primarily spouses or co-habitants of applicants. Some records also included findings from interviews conducted by background investigators and approximately 5.6 million included fingerprints. Usernames and passwords that background investigation applicants used to fill out their background investigation forms were also stolen. Also, in early 2015, OPM discovered that the personnel data of 4.2 million current and former Federal government employees had been stolen. This means information such as full name, date of birth (DOB), home address, and SSNs were affected.[8]

In February 2022, the GPO Director testified about privacy management at a hearing before the Committee on House Administration. To paraphrase some of his points, GPO is entrusted with PII belonging to its employees, customers, and, by nature of its business, the general public. Changes in technology have driven concern about the ease with which personal information, such as names and addresses, is available. The threat from the use of that information, paired with certain details, such as DOB and SSN, has also exponentially increased.[9]

Objectives

Our overall objective was to review the GPO Privacy Program's effectiveness and efficiency, through the below sub-objectives:

- Determine if GPO policies governing the Privacy Program are aligned to Federal regulations and best practices.
- Quantify to what extent GPO collects, uses, stores, retains, and disposes of PII.
- Evaluate GPO's response to any privacy breaches that occurred within the past three years (2018 - 2020).
- Evaluate the effectiveness and efficiency of GPO's Privacy Program implementation.

Prior OIG Coverage

GPO OIG 19-0002-1, *Suspension/Debarment Referral*, December 19, 2019. In this incident, a contractor mishandled PII information under their control while performing a contract. This contractor was later debarred from working as a contractor for GPO.

[8] OPM Cybersecurity Resource Center Cybersecurity Incidents
[9] "Big Data: Privacy Risks and Needed Reforms in the Public and Private Sectors" Testimony before the Committee on House Administration, February 16, 2022.

Criteria

- *The Privacy Act of 1974*, as amended, 5 United States Code (U.S.C.) Section 552a (Privacy Act)
- *E-Government Act of 2002* (E-Gov Act)
- Office of Management and Budget (OMB) Memorandum M-16-14, *Category Management Policy 16-2: Providing Comprehensive Identity Protection Services, Identity Monitoring, and Data Breach Response*, July 1, 2016
- OMB Memorandum M-17-06, *Policies for Federal Agency Public Websites and Digital Services*, November 8, 2016
- OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*, January 3, 2017
- National Institute of Standards and Technology (NIST) Special Publication 800-84, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*, September 2006
- NIST Special Publication 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, April 2010
- GPO Directive 705.28B, *Information Technology Systems Development Life Cycle Policy*, October 22, 2019
- GPO Directive 705.35, *Information Technology Electronic Equipment Disposal (e-Waste) Policy*, September 8, 2020
- GPO Directive 825.33C, *Information Technology (IT) Security Program Statement of Policy*, March 19, 2021
- GPO Directive 825.41A, *Privacy Program: Protection of Personally Identifiable Information (PII)*, June 12, 2015 (SUPERSEDED)
- GPO Directive 825.41B, *Privacy Program: Protection of Personally Identifiable Information (PII)*, April 06, 2021
- GPO Directive 840.1B, *GPO Records Management Program*, February 28, 2018
- GPO Directive 840.7A, *GPO Comprehensive Records Schedule*, September 2, 2014
- GPO Privacy Incident Handling Guidance (PIHG), Version 5.0, June 10, 2020
- GPO Privacy Incident Response Team (PIRT) Framework and Procedures, Version 6.0, April 24, 2020

Supplemental Background

U.S. Privacy Governance

According to some privacy experts, the U.S. Constitution does not explicitly articulate rights to privacy, but there are aspects of privacy that are explicitly and implicitly called out.[10] For example, the Fourth and Fifth Amendments protect against unreasonable search and seizure and the protection against self-incrimination. As with the Constitution,

[10] U. S. Government Privacy: Essential Policies and Practices for Privacy Professionals, International Association of Privacy Professionals. Julie McEwen, Stuart Shapiro. (2009).

there is no overarching privacy legislation, but there are significant laws that protect aspects of privacy.[11] Below are two privacy laws that are most germane to this report, but are not an all-inclusive summary of U.S. privacy legislation.

The Privacy Act of 1974, as amended, 5 U.S.C. Section 552a. The purpose of the Privacy Act, broadly stated, is to balance the government's need to maintain information about individuals with the rights of individuals to be protected against unwarranted invasions of their privacy stemming from federal agencies' collection, maintenance, use, and disclosure of personal information about them. The historical context of the Privacy Act is important for understanding its remedial purposes. In 1974, Congress was concerned with curbing the illegal surveillance and investigation of individuals by federal agencies that were exposed during the Watergate scandal. Congress was also concerned with potential abuses presented by the government's increasing use of computers to store and retrieve personal data by means of a universal identifier – such as an individual's SSN. The Privacy Act focuses on four basic policy objectives:

1. To restrict disclosure of personally identifiable records maintained by agencies.
2. To grant individuals increased rights of access to agency records maintained on themselves.
3. To grant individuals the right to seek amendment of agency records maintained on themselves upon a showing that the records are not accurate, relevant, timely, or complete.
4. To establish a code of "practices" that requires agencies to comply with statutory norms for the collection, maintenance, and dissemination of records.[12]

The E-Government Act of 2002. This law was enacted to improve the use of information technology (IT) and promote electronic government services, but it also introduced privacy protections for Federal IT systems. Section 208 of the E-Gov Act has two privacy-centric provisions, Sections 208(b) and 208(c). The first provision requires the completion of a privacy impact assessment (PIA) for all new IT systems, or when major changes are made to existing systems. PIAs identify and mitigate privacy risks of the information system, more fully described below. The second provision requires agencies to maintain privacy policies on their websites and in machine readable format.

Broadly, the E-Gov Act requires Federal agencies to conduct PIAs when:

- Developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form; or
- Initiating a new collection of information that:
  - Will be collected, maintained, or disseminated using information technology; and
  - Includes any information in an identifiable form permitting the physical or online contacting of a specific individual, if identical questions have been

[11] U. S. Government Privacy: Essential Policies and Practices for Privacy Professionals, International Association of Privacy Professionals. Julie McEwen, Stuart Shapiro. (2009).
[12] United States Department of Justice Overview of the Privacy Act of 1974, 2015 Edition

posed to, or identical reporting requirements imposed on, 10 or more persons, other than agencies, instrumentalities, or employees of the Federal Government.

The E-Gov Act also requires the publication of PIAs, which must analyze and describe the following information:

- What information is being collected.
- Why the information is being collected.
- The intended use of the information.
- With whom the information will be shared.
- What opportunities individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how individuals can grant consent.
- How the information will be secured.
- Whether a system of records is being created under the Privacy Act.
- What choices the agency made regarding an information system or collection of information as a result of performing the PIA.

GPO Privacy Governance

GPO Directive 825.41B, *Privacy Program: Protection of Personally Identifiable Information*, April 06, 2021. This directive details the policies, processes, best practices, and training required to guide GPO employees and contractors to protect PII during all stages of the information lifecycle: when collecting, storing, using, disseminating, or disposing of PII. The directive further highlights responsibilities for safeguarding PII on both the organizational and individual levels and states the penalties for not complying with the Privacy Program. GPO's goal is to protect PII because the loss, compromise, or unauthorized disclosure of PII may potentially lead to identity theft or other fraudulent use that could result in substantial harm, embarrassment, inconvenience, or unfairness to the affected individuals and tarnish the agency's reputation.

The responsibilities defined in GPO Directive 825.41B include:

a. The Privacy Officer has the overall responsibility and authority to devise and implement the needed protective measures and is to be assisted by the Office of General Counsel (OGC), IT management, and BUs in implementing the directive.
b. GPO OGC assists the Privacy Officer in clarifying the applicability of a particular law, regulation, or other mandates.
c. Senior managers of each BU are responsible for assisting the Privacy Office in implementing the policy within the BU.
d. All GPO employees and contractors are responsible for:
    - Ensuring the accuracy, relevance, timeliness, and completeness of records.
    - Collecting only the required authorized PII directly from the individual whenever possible or from existing GPO information systems.

- Maintaining and using records with care to prevent any inadvertent disclosure of information protecting PII from unauthorized disclosure or misuse.
- Reporting to the Privacy Officer any known or suspected instance of unauthorized access or improper disclosure of PII within GPO, or by a contractor or subcontractor handling GPO procured contracts.

Privacy Incident Response Team (PIRT) Framework and Procedures. These procedures focus on incident response and notification protocols, both internal and external. They include notifications to the GPO Inspector General, GPO Computer Security Incident Response Team (CSIRT), and the United States Computer Emergency Readiness Team (US-CERT), as appropriate. GPO officials including the BU Director, BU Privacy Points of Contact (PPOCs), and the Privacy Officer have key roles in handling the privacy incident. BU PPOCs are GPO employees supporting the BUs. PPOCs work with leadership to address issues related to PII and ensure collected PII is authorized. The privacy incident reporting process sequentially follows seven tiers, below, and is to be completed within 24-48 hours of notification of the incident.

Tier 1 – Reporting the Incident
Tier 2 – Creating the Preliminary Written Report
Tier 3 – Assess the Risk of Harm
Tier 4 – Escalation to External Authorities
Tier 5 – Risk Containment
Tier 6 – Mitigation Processes
Tier 7 – Incident Closure

Privacy Incident Handling Guide (PIHG). GPO's PIHG is directed to BU Managing Directors and PPOCs; it defines the BU obligation to protect PII, the procedures to respond to a potential loss or compromise of PII, and the required protocols for reporting any breaches or compromise of PII to the GPO PIRT. It is arranged as a Frequently Asked Questions, or question and answer, format. It defines what a privacy incident is, who is responsible for reporting it, and gives an overview of the PIRT Tiers.

INSPECTION RESULTS

Finding 1. GPO states that its Privacy Program is aligned with Federal law and oversight guidance, specifically from the Privacy Act, the Office of Management and Budget (OMB), and the National Institute of Standards and Technology (NIST). However, GPO omits the inclusion of Systems of Records Notices, a basic privacy practice from the Privacy Act. GPO also lacks transparency in what privacy laws and guidance it follows and why.

According to GPO's privacy website, GPO places a high priority on protecting PII and has aligned its Privacy Program directive to federal law and oversight guidance as best practices.[13] While as a Legislative branch agency, GPO is not required to follow federal laws designed to govern the Executive branch, GPO generally adheres to U.S. privacy governance, including OMB and NIST guidance. However, GPO does not specifically detail what federal laws and guidance they do follow in all cases nor the bases for their deviations from federal best practices. Of particular concern is GPO's omission of the Privacy Act's SORN requirement, an otherwise standard privacy practice within the federal government. Therefore, GPO's Privacy Program falls short of a thorough privacy program where PII is protected during all stages of the information life cycle, creating the possibility of PII loss, compromise, or unauthorized disclosure.

Criteria

- *The Privacy Act of 1974*, as amended, 5 U.S.C. Section 552a
- OMB Memorandum M-16-14, *Category Management Policy 16-2: Providing Comprehensive Identity Protection Services, Identity Monitoring, and Data Breach Response*, July 1, 2016
- OMB Memorandum M-17-06, *Policies for Federal Agency Public Websites and Digital Services*, November 8, 2016
- OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*, January 3, 2017
- NIST Special Publication 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, April 2010
- GPO Directive 825.41B, *Privacy Program: Protection of Personally Identifiable Information (PII)*, April 06, 2021

GPO's Privacy Program Directive References Select Federal Law and Oversight Guidance

We asked GPO the following question, "as a Legislative Branch Agency, what laws and or regulations govern GPO's Privacy Program?" GPO responded that it is not subject to the

[13] https://www.gpo.gov/privacy

Privacy Act or the E-Government Act, but that it has drawn from those statutes, their implementing regulations, and other regulatory materials, and established a privacy program in compliance with federal regulations, as best practices. GPO's privacy website reiterates that answer stating, "Note that as a Legislative branch agency GPO is not required by law to adhere to the requirements and oversight guidance, but the Agency has recognized the requirements and oversight guidance as a best practice." GPO Directive 825.41B*, Privacy Program: Protection of Personally Identifiable Information (PII)*, April 06, 2021, promulgates policies, processes, best practices and training required, guiding the workforce to protect PII, including PHI, during all stages of the information lifecycle.

Directive 825.41B references one federal law and four guidance documents as best practices applicable to GPO's Privacy Program:

1. *The Privacy Act of 1974*, as amended, 5 U.S.C. Section 552a. The directive states that GPO uses the fair information practice principles from the Privacy Act. Examples of these principles include transparency, individual participation, limited use, accountability, and auditability of PII. The Privacy Act also introduces the requirement for federal agencies to notify the public, via the federal register, of the PII they manage. This notification is called a System of Records Notice (SORN).[14] GPO does not create nor publish SORNs. As a SORN is intended to inform the public about what kinds of PII federal agencies maintain, GPO's assertion that it adheres to the fair information practice principles of the Privacy Act is incongruent.

System of Records Notice (SORN):

A system of records is a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifier assigned to the individual. The Privacy Act requires each agency to publish notice of its systems of records in the Federal Register. This notice is generally referred to as a SORN.

2. OMB Memorandum M-16-14, *Category Management Policy 16-2: Providing Comprehensive Identity Protection Services, Identity Monitoring, and Data Breach Response*, requires that when agencies need identity protection services, using the government-wide blanket purchase agreements for identity monitoring data breach response and protection services awarded by the General Services Administration addresses that requirement. GPO signed a one-year contract with an identity monitoring protection service provider on July 30, 2021. According to the Privacy Officer, the scope of the protection is for GPO employees and their identities.
3. OMB Memorandum M-17-06, *Policies for Federal Agency Public Websites and Digital Services*, requires agencies to be transparent about policies and practices with respect to PII. This includes maintaining an up-to-date Privacy Program Page on an agency's principal website, and posting plain language privacy policies on an

[14] Privacy Act, Office of Privacy and Open Government, U.S. Department of Commerce (doc.gov)

agency's website. The GPO Privacy Program website includes an overview of its program, as well as its authority, policy references, and more.[15] However, the website does not clearly and definitively enumerate which policies GPO follows.

4. OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*, provides Federal policy regarding preparing for and responding to a breach of PII. GPO Directive 825.41B applied this guidance through the implementation of two Incident Response Plan documents, the PIRT Framework and Procedures and the PIHG.
5. NIST Special Publication 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, references the E-Gov Act and its requirement to conduct PIAs. PIAs should address risk at every stage of the system development life cycle.

Further, the GPO Director testified that GPO "devote[s] considerable time, attention, and resources to securing and protecting [PII]" as "[r]obust protection of PII is critical to building trust with [GPO] customers and stakeholders."[16]

The GPO Privacy Program directive references selected federal law and oversight guidance as best practices. However, GPO's reasoning for deviating from widely practiced federal privacy laws, such as SORN requirements from the Privacy Act, while adhering to some, but not all, of those practices, is not explained. Given that the "best practice" acknowledged by GPO is the OMB and NIST standard, their omission of key aspects means their program is, by definition, incomplete. GPO's Privacy Program falls short of a thorough privacy program where PII is protected during all stages of the information life cycle, thereby creating the possibility of PII loss, compromise, or unauthorized disclosure.

Recommendation 1. Identify the federal privacy laws and oversight guidance, and their applicable sections, that GPO intends to follow as definitive guidance. Include the reasoning and/or basis for those determinations.

Management Comments

GPO concurred with this recommendation. GPO stated that in establishing GPO's Privacy Program, GPO researched Federal laws and guidance available from OMB, NIST, and the National Archives and Records Administration, and studied privacy programs of various Government agencies.

GPO stated the goal of this research was to include the laws and guidance that demonstrated practices to best implement a robust privacy program at GPO. GPO determined the laws and guidance previously identified in the above section best applied to its privacy program scope and activities, as referenced in GPO Directive 825.41B, *Privacy Program: Protection of Personally Identifiable Information (PII)*, April 06, 2021.

[15] https://www.gpo.gov/privacy
[16] "Big Data: Privacy Risks and Needed Reforms in the Public and Private Sectors" Testimony before the Committee on House Administration, February 16, 2022.

In accordance with this recommendation, GPO will revisit other OMB and NIST guidance and standards and evaluate how GPO can further strengthen its Privacy Program.

OIG Response

GPO's concurrence and planned actions are partially responsive to this recommendation.

In addition to OMB and NIST guidance and standards, the Federal Privacy Council website lists multiple federal privacy laws and oversight guidance that GPO could review for best practices to strengthen GPO's Privacy Program.[17] We look forward to receiving GPO's evaluation that includes the reasoning and/or basis for determining which definitive privacy guidance GPO follows. In order to close this recommendation, the agency must identify the specific sections of the laws and guidance that best apply to its privacy program, as referenced in GPO Directive 825.41B. Additionally, the agency must identify all of the federal privacy laws and oversight guidance that it considered and reviewed, and the reasoning and/or basis for determining which definitive privacy guidance the agency follows.

[17] www.fpc.gov

Finding 2. GPO needs to improve recordkeeping and PII management compliance for the 24 PII systems identified.

During our review, we found that the Privacy Officer was aware of 19 GPO PII systems that collect, use, store, and retain PII; but was unaware of five additional PII systems used by the BUs. GPO was unable to produce PII confidentiality impact levels for these systems, and had not created compliance documents for all PII systems. Since 2017, GPO has not conducted any Privacy Compliance Reviews (PCRs) for the systems that collect, use, and store PII. Further, the directive governing retention and disposal of records does not include guidance on the identification of records containing PII. Without identifying the confidentiality impact level, maintaining compliance documents, and conducting PCRs, GPO risks failing to design and implement appropriate safeguards to protect PII, and the systems that contain PII, from unauthorized access or disclosure.

Criteria:

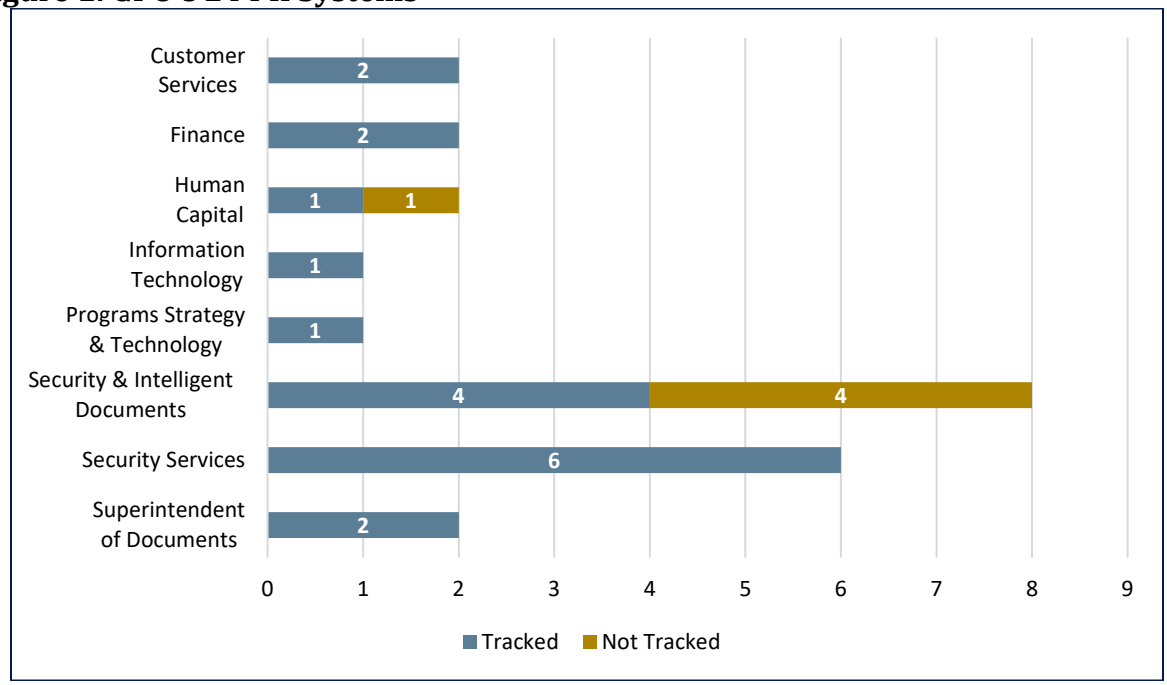
- GPO Directive 705.35, *Information Technology Electronic Equipment Disposal (e- Waste) Policy*, September 8, 2020
- GPO Directive 825.41A, *Privacy Program: Protection of Personally Identifiable Information (PII)*, June 12, 2015 (SUPERSEDED)
- GPO Directive 825.41B, *Privacy Program: Protection of Personally Identifiable Information (PII)*, April 06, 2021
- GPO Directive 840.1B, *GPO Records Management Program*, February 28, 2018
- GPO Directive 840.7A, *GPO Comprehensive Records Schedule*, September 2, 2014

PII Lifecycle Management and Documentation for 19 of 24 PII Systems

GPO's Privacy Program directive requires that information systems are protected from unauthorized PII disclosure, such as access, modification, disruption, or destruction; that compliance with protecting those systems is assessed through compliance documents; and that the Privacy Officer schedules biennial periodic reviews of PII held by all BUs.

Through these activities, the GPO Privacy Officer tracks the collection, use, storage, and retention of PII for 19 systems. GPO BUs identified five additional GPO PII systems that were not reported to, and therefore not tracked by, the Privacy Officer; see Figure 1, below.

Figure 1: GPO's 24 PII Systems



Source: OIG analysis of GPO Data.

As shown in Figure 1, one of the five untracked systems is managed by Human Capital. The other four untracked systems are managed by Security & Intelligent Documents.

The Human Capital system, HC Dashboard, is an internal website that provides users with a comprehensive method to address their Human Capital needs, as described below. The HC Dashboard can have a multitude of PII ranging from names, addresses, phone numbers, salary, and retirement information.

- **HC Dashboard**, which has several modules to help managers:
  - Submit OPM Standard Form 52, Request for Personnel Action
  - Obtain real-time status of all hiring and non-hiring actions
  - Develop and complete annual performance plans and ratings
  - Determine excepted and emergency designations
  - Obtain information on various Human Capital policies and programs

The four untracked Security & Intelligent Documents systems all create Identification Cards (ID), which display PII such as the name and photograph of the cardholder. The ID cards are created to support unique applications located at other agencies and are described below.

- **U.S. Asia-Pacific Economic Cooperation (APEC) Business Travel Card (ABTC) Program.** The APEC is an economic forum comprised of 21 members including the United States and Canada, with the primary goal of supporting sustainable economic growth and prosperity in the Asia-Pacific region. One of APEC's initiatives is the ABTC Program. The ABTC Program is a voluntary program that

enables qualified U.S. business travelers or U.S. government officials who are engaged in APEC business or business in the APEC region the ability to gain access to fast-track immigration lanes at participating airports in the 20 foreign APEC member economies.

- **District of Columbia (DC) One Card ID** is a consolidated credential designed to give children, adults and seniors access to DC government facilities and programs, including public schools, recreation centers, libraries, and public transit. The DC One Card is also a building access card for DC government employees and includes Metro SmarTrip® capability for travel within the Washington Metropolitan Area Transit Authority transportation system.

- **Pentagon Contractors ID Card** is a form of Department of Defense Common Access Card, specifically for contract employees of the Pentagon. A Common Access Card is generically described as a "Smart" ID card for active-duty military personnel, Selected Reserve, Department of Defense civilian employees, and eligible contractor personnel.

- **Transportation Worker Identification Credential**, also known as **TWIC®**, is required by the Maritime Transportation Security Act for workers who need access to secure areas of the nation's maritime facilities and vessels. The Transportation Security Administration conducts a security threat assessment, i.e., a background check, to determine a person's eligibility and issues the credential. U.S. citizens and immigrants in certain immigration categories may apply for the credential. Most mariners licensed by the U.S. Coast Guard also require a credential.

Lack of PII Confidentiality Impact Levels

According to the Privacy Program directive, PII must be evaluated to determine a confidentiality impact level. Information systems are secured based on the confidentiality impact level rating: low, moderate, or high. The rating indicates the potential harm that could result from inappropriately accessed, used, or disclosed PII.

The background section of this report defines PIAs, specifically that PIAs should document the analysis and description of how PII is secured. GPO provided the PIAs for 19 systems; none included a confidentiality impact level. Moreover, the BU PPOCs and the Privacy Officer did not have PIAs, with associated confidentiality impact levels, for the five untracked systems.

Without identifying the PII confidentiality level, the appropriate safeguards cannot be designed and implemented. While GPO's Privacy Program directive requires determining a confidentiality impact level, the directive does not state where this information is to be recorded. Documenting the PII confidentiality levels, and identifying where the levels are recorded, is supported by the Director's recent testimony that "GPO has sought to follow

the recommendations [of] the National Institute of Standards and Technology (NIST)" including categorizing PII by confidentiality impact level and applying the appropriate safeguards based on them.[18] Without clearly identifying the confidentiality impact level, GPO risks failing to design and implement appropriate safeguards to protect PII.

Lack of Compliance Documentation for PII Systems

The primary method of assessing BU compliance with the Privacy Program directive is through the use of compliance documentation, including:

- **Privacy Threshold Analysis (PTA)**: Identifies the justification and authority for using sensitive PII within an information system or hardcopy workflow. The PTA is waived if the system owner opts to directly submit a PIA.
- **Privacy Impact Assessment (PIA)**: Required for projects that use PII to determine the risk to privacy, including collection, use, sharing, retention, notice of sharing, and access, redress, and correction.
- **System Disposal Assessment (SDA)**: Documents if PII is at the end of lifecycle and no longer being transmitted due to an information system being retired. If PII is not needed, it must be securely expunged. PII held on hardware equipment holding must become permanently non-retrievable.

We requested all compliance documents for the PII systems, including PTAs, PIAs, and SDAs. However, while there were PIAs for 19 of the 24 PII systems, we received the PTA for only one system and did not receive any SDAs. The lack of SDAs is particularly concerning, as one PII system was retired in fiscal year 2019,[19] and a second system no longer collects PII.[20] Without the SDAs, GPO has no record that the system's associated PII was securely handled. Without maintaining these compliance documents, GPO cannot assess its efforts to protect PII.

In addition to developing and maintaining compliance documentation, the BUs are to maintain and share with the Privacy Officer a complete listing, or inventory, of all PII used. However, the BUs did not have a listing of the PII systems used. Maintaining and sharing a complete inventory listing of all PII used with the Privacy Office is one way to ensure BU compliance with the Privacy Program directive. Without a complete listing of their PII systems, the BUs and Privacy Officer, and therefore GPO, risk failing to identify and protect the confidentiality of PII under its control.

---

[18] "Big Data: Privacy Risks and Needed Reforms in the Public and Private Sectors" Testimony before the Committee on House Administration, February 16, 2022.

[19] The Federal Digital System (FDsys), which provided free online access to official Federal Government publications and securely controls digital content throughout its lifecycle to ensure content integrity and authenticity, guarantees long-term preservation and access to digital Government content. FDsys was replaced by **govinfo**.

[20] The Procurement Information Control System, an application that captures the receipt of order data from GPO customers, such as federal agencies, and tracks the status of the jobs associated with those orders.

Lack of Privacy Compliance Reviews

Per GPO Directive 825.41B, GPO aims to protect its PII systems through PCRs and biennial periodic reviews of PII held by all BUs.

The PCRs are used to determine if any gaps in privacy compliance policy have been created by changes to internal data flows or collections, alteration of a business process, significant new uses or disclosures of PII information, or implementation of new information systems. PCRs are to be conducted collaboratively by the GPO Privacy Officer and the BU PPOCs once every 2 years.

We requested evidence supporting prior PCRs, but the information was not provided. The Privacy Officer informed us that the January 2021 PCR was postponed "in light of" this OIG inspection. The Privacy Officer further explained they "did not want to inundate… Business Unit managers and privacy point of contacts [sic] for the similar information… being gathered" for the OIG inspection. However, the Privacy Officer served in this role since 2017 and did not provide any evidence of PCRs being completed in the four previous years, 2017-2020. Without PCRs, we question how the Privacy Officer can determine if there are any gaps in privacy compliance policy, leaving GPO vulnerable to the risk that PII is not appropriately safeguarded. Indeed, this inspection revealed there are gaps in privacy compliance policy, as the Privacy Officer does not have PTAs or PIAs for all of GPO's systems, and does not have SDAs for the systems that have retired.

The schedule for biennial periodic reviews of PII is maintained by the Privacy Officer and coordinated with the BU PPOCs.[21] GPO's updated Directive 825.41B added the requirement in 2021 that these periodic reviews would be biennial. According to the Privacy Officer, biennial periodic reviews and PCRs are interrelated and the biennial reviews become a part of the PCR. Since this is a relatively new requirement, we highlight that while the directive does not define specifically what a biennial review is or does, conducting biennial reviews is another way to confirm that both the BUs and the Privacy Officer are aware of the inventory of PII used by the BUs.

In summary, the GPO privacy information provided did not identify PII confidentiality impact levels. Further, GPO did not maintain and assess compliance documents and did not conduct biennial PCRs. Without doing so, GPO risks ensuring it identifies and protects PII, and the systems that contain PII, from unauthorized access or disclosure.

PII Disposal Guidance can be Improved.

GPO Directive 840.7A, *GPO Comprehensive Records Schedule*, September 2, 2014, defines the records schedule maintenance and disposition, or destruction, for all records created and maintained at GPO, by all GPO operating units and divisions, regardless of media type, i.e., paper or electronic. Directive 840.7A provides authorized disposition

[21] The original GPO Directive 825.41A only required a "periodic review," whereas the updated 2021 GPO Directive 825.41B requires "biennial periodic reviews."

instructions for records within the scope of the schedule. The records schedule is largely arranged around the BU functions and includes a retention period stating when the records can be destroyed. GPO Directive 840.1B, *GPO Records Management Program*, February 28, 2018, ensures that appropriate documents are saved until their scheduled disposition, and uses GPO Form 1350 *Records Transmittal and Receipt* to transfer records internally and to destroy records.

GPO's Records Administration & Management Division has a database for tracking records, and a means to destroy paper records with PII. The Division Chief told us that most GPO records are now digital, and instead of sending them to the Records Administration & Management Division for safeguarding and eventual disposal, BUs maintain the records in their office space. The paper records that are turned over to the GPO Records Administration & Management staff are stored in a locked room and tracked by title in a Records Administration & Management Inventory.

The Division Chief stated that in 2020 (approximately), records containing PII were marked at the time of transfer. However, more than a year later, the records database did not reflect a space to indicate if the records contain PII. Further, the documents transferred prior to 2020 did not identify if they contained PII. GPO should review its stored records to identify and mark which records contain PII.

Directive 840.1B does not stipulate that records containing PII be identified, and the GPO Form 1350 does not have a space to clearly indicate if any of the transferred records contain PII. This contrasts with the Records Administration & Management Division Chief's assertion that PII is identified at the time of transfer. To ensure PII records are properly protected, GPO's records management directive and the corresponding GPO Form 1350 should clearly state that records transferred to Records Administration & Management for storage and destruction must indicate whether or not the records contain PII.

Finally, while GPO's Privacy Program directive states records are to be retained in accordance with the Records Schedule directive, the Privacy Program directive does not identify how users or BUs are to dispose of PII documents or information systems. Specifically, while the SDA description references making electronic data permanently non-retrievable by means stated in GPO Directive 705.35, *Information Technology Electronic Equipment Disposal (e-Waste) Policy*, September 8, 2020, the Privacy Program directive does not include a responsibility to ensure the proper destruction of PII documents or information systems; nor does the e-Waste directive.[22] Without oversight for the destruction, or disposal, of all media types that contain PII, the Privacy Officer may not be able to establish a framework and measures to protect PII from unauthorized use, access, disclosure, or sharing during its entire lifecycle, from creation through destruction. GPO should ensure the Privacy Program includes protecting PII even during its destruction.

[22] We previously reported Inspection Report Number 20-09, GPO's Electronic Waste (e-Waste) Processes and Procedures, September 10, 2020.

In summary, the Privacy Officer cannot assist GPO in the design and implementation of safeguards and privacy controls for systems not currently tracked. In addition, the absence of PCRs and PII inventory and reporting exposes GPO to privacy risks and lack of protection of PII from unauthorized access, use, and disclosure; thereby, resulting in potential harm to individuals or the agency and its information systems.

Recommendation 2. Develop PIAs for the five untracked PII systems identified: HC Dashboard, APEC ABTC, DC One Card ID, Pentagon Contractors ID Card, and TWIC®.

Management Comments

GPO concurred with this recommendation. GPO will develop PIAs for the HC Dashboard, APEC ABTC, DC One Card ID, Pentagon Contractors ID Card, and TWIC®.

OIG Response

GPO's concurrence and planned actions are responsive to this recommendation. In order to close this recommendation, the agency must provide PIAs for the HC Dashboard, APEC ABTC, DC One Card ID, Pentagon Contractors ID Card, and TWIC®.

Recommendation 3. Identify the mechanism to document confidentiality impact levels and document the confidentiality impact levels for all GPO PII systems.

Management Comments

GPO concurred with this recommendation. GPO noted that Finding 3 of the draft report states, "GPO's privacy incident response procedures should incorporate NIST Special Publication 800-122 in order to provide more detailed implementation guidance when responding to privacy incidents and breaches." GPO stated its current PIRT Framework and Procedures actually refer to NIST eight times, and that the mechanism suggested in this recommendation for documenting confidentiality impact levels is illustrated in Section 3 of the PIRT Guide. However, GPO will update the PIRT Guide, as necessary, to further elaborate on applicable guidelines included in NIST Special Publication 800-122.

GPO will collaborate with BU Managers to update the inventory of PII for each of the 19 GPO systems carrying PII. GPO will then conduct the PIRT documented process to establish the confidentiality impact level for each system and update each PIA to reflect the confidentiality impact level.

OIG Response

GPO's concurrence is responsive to this recommendation, as is its planned action to update the PIA of each PII system to reflect the confidentiality impact level.

However, allow us to provide clarification regarding our position on GPO's assertion that Section 3 of the PIRT Framework and Procedures illustrates how to document confidentiality impact levels. The PIRT Framework and Procedures is a document that focuses on incident response. Section 3 of the PIRT Framework and Procedures is titled "Risk of Harm Assessment." At this stage of an incident response, the specific incident's risk of harm is assessed, which then determines which entity within GPO will be responsible for investigating, producing notifications, and mitigating the risk.

Conversely, confidentiality impact levels determine how an information system with PII is to be secured, and the appropriate safeguards that can be applied to the PII. According to NIST Special Publication 800-122, organizations "should decide which factors it will use for determining impact levels and then create and implement the appropriate policy, procedures, and controls."

Thus, confidentiality impact levels proactively identify how to keep PII safe from an incident, while GPO's referenced Risk of Harm Assessment reactively determines how to respond to an incident where PII was not kept safe.

In order to close this recommendation, the agency must provide the PIA for each PII system, reflecting the confidentiality impact level. Additionally, the agency must update the Privacy Program directive to reflect where and how confidentiality impact levels are to be documented.

Recommendation 4. Implement a process to conduct BU PII inventories and share the results with the Privacy Officer.

Management Comments

GPO concurred with this recommendation. GPO highlighted that as stated in GPO Directive 825.41B, Section 9.e – Business Unit's PII Activities, GPO surveys each BU to inventory PII captured by the BU. The next survey is scheduled for September 2022. The Privacy Office distributes a spreadsheet with instructions to the BUs for submitting the PII used in the BU and for submitting any plans the BU has to curtail the use of PII. GPO shared an account of all BU PII Holdings as part of the Data Call Documents with the OIG through SharePoint on March 3, 2021.

OIG Response

GPO's concurrence and planned actions are responsive to this recommendation.

We acknowledge the information shared with the OIG, in response to our request for "[a] detailed accounting of the GPO PII holdings." The information included an email from the Privacy Officer regarding "PII Data Collection," and asked the recipient "for a favor" of filling out a spreadsheet to make information current. The spreadsheets contained a question asking if PII was still being collected, stored, or processed, and if there were any new items. The spreadsheet guidance also stated to select a "Yes/No" response. Our

review of the information provided revealed that the spreadsheets were only identified by BU, and did not name any of the PII systems. In addition, two of the ten responding BUs responded with information other than the requested "Yes/No." We were unable to use the information in the spreadsheets to identify the PII systems used by the BUs.

We reiterate that the BUs maintenance of a complete inventory listing of all PII used, and sharing that inventory with the Privacy Office, is one way to ensure BU's compliance with the Privacy Program directive.

In order to close this recommendation, the agency must provide the complete listing of all PII used in the BUs, and documentation of how each BU inventory listing is shared with the Privacy Officer. If, as the agency stated in its management comments that surveying each BU is a Privacy Officer responsibility, the Privacy Program directive needs to be updated to reflect this, and the agency needs to provide evidence that the survey conducted by the Privacy Officer includes the names of each PII system and any changes to the PII systems.

Recommendation 5. Conduct biennial Privacy Compliance Reviews in accordance with GPO's Privacy Program directive.

Management Comments

GPO concurred with this recommendation. GPO plans to commence biennial PCRs in August 2022. GPO intends to hire a Junior Privacy Officer who will assist the Privacy Officer with these compliance reviews.

OIG Response

GPO's concurrence and planned actions are responsive to this recommendation. In order to close this recommendation, the agency must provide evidence of biennial Privacy Compliance Reviews.

Recommendation 6. Review all stored records to identify and mark which records contain or may contain PII.

Management Comments

GPO concurred with this recommendation. GPO's Privacy Office is collaborating with the Records Management unit to develop a process for inspecting and marking existing records that may contain PII. This includes modifying the current database for capturing metadata regarding PII, and inspecting and marking all hard copy boxes in Records Management's possession to reflect the presence of PII. GPO will update the revised database to reflect the presence of PII in records.

GPO is also preparing a Statement of Work to acquire and implement an Electronic Records Management system to facilitate inventorying, housing, and managing GPO

records. GPO expects that the metadata captured for GPO records will facilitate PII tracking, management, and redaction as required.

OIG Response

GPO's concurrence and planned actions are responsive to this recommendation. In order to close this recommendation, the agency must provide the process for inspecting and marking existing records, the updated database that reflects the presence of PII in records, and the implemented Electronic Records Management system.

Recommendation 7. Update the Records Management Program directive and the corresponding GPO Form 1350 to clearly state that records transferred to Records Administration & Management Division, for storage and destruction, must indicate whether or not the records contain PII.

Management Comments

GPO concurred with this recommendation. GPO stated it recently revised GPO Directive 840.1B, Records Management Program, and GPO Form 1350, Records Transmittal and Receipt. The updated form includes the capability to mark the presence of PII in the records being transferred. GPO anticipates approval and publishing of the updated directive and form.

OIG Response

GPO's concurrence and planned actions are responsive to this recommendation. In order to close this recommendation, the agency must publish the updated Records Management Program directive and corresponding GPO Form 1350.

Finding 3. GPO's privacy incident response procedures should incorporate NIST Special Publication 800-122 in order to provide more detailed implementation guidance when responding to privacy incidents and breaches.

GPO's Privacy Program includes a process to identify, report, investigate, and respond to privacy incidents. However, GPO's PII Incident Response Plans do not include NIST Special Publication 800-122 guidance, omitting essential steps in implementing incident response, such as instructions on how to notify appropriate individuals and organizations. Without thorough Incident Response Plans, GPO risks failing to adequately evaluate and respond to suspected PII breaches.

Criteria

- OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*, January 3, 2017
- NIST Special Publication 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, April 2010
- GPO Directive 825.41B, *Privacy Program: Protective of Personally Identifiable Information (PII)*, April 06, 2021
- GPO Privacy Incident Handling Guidance (PIHG), Version 5.0, June 10, 2020
- GPO Privacy Incident Response Team (PIRT) Framework and Procedures, Version 6.0, April 24, 2020

GPO Privacy Office Incident Reporting and Response Plans

GPO's Privacy Program includes a process to identify, report, investigate, and respond to privacy incidents. The process follows GPO's PIRT Framework and Procedures and is supplemented by the PIHG, both of which were previously described in the Background section of this report.

GPO's Privacy Program directive references OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of PII*, as providing guidance to prepare for and report a breach of PII. OMB defines a privacy incident as an occurrence that (1) jeopardizes the integrity, confidentiality, or availability of information or an information system; or (2) violates or imminently threatens the violation of law, security policies, security procedures, or acceptable use policies. OMB defines a breach as a type of incident, where PII is actually compromised, such as through an unauthorized disclosure or similar occurrence, because (1) a person other than an authorized user accesses or potentially accesses PII, or (2) an authorized user accesses or potentially accesses PII for an unauthorized purpose.

GPO's Privacy Data Breaches

GPO's Privacy Officer received reports of ten privacy incidents between 2018 and 2020; GPO qualified seven as privacy data breaches. All seven privacy data breach incidents originated from the GPO Customer Services BU and their contractors. The Customer Services BU provides a comprehensive suite of services to ensure a coordinated contracting and printing process for its customers. Services are provided through strategic teams that provide direct assistance to assigned customers, through offices nationwide that provide a network of regional coverage, and through various procurement vehicles to satisfy specific printing needs. The contractors handled and processed PII on behalf of GPO's customers. GPO records revealed that the incidents were reported, and GPO worked with the contractors and the customers, to identify a satisfactory resolution for the incidents. Table 1 details GPO's seven privacy data breaches.

Table 1. Privacy Data Breach Incidents

Date of Notice	Reported By	Type of PII	PII Location
02/08/2018	Customer Agency	Name, DOB, SSN	Wage & Earning Statements
12/21/2018	Contractor	Name, DOB, SSN	File folders in boxes
02/12/2019	Customer Agency	Name, Address	Website with estate information
03/19/2019	Customer Agency	Name, DOB	The contractor sent PII via unprotected email
06/07/2019	Customer Agency	Name, Address, Unique ID number	ID cards
10/23/2019	Contractor	Addresses	Mail list of points of contact
11/14/2019	Customer Agency	Name, Address, Unique ID number	ID cards

Source: GPO

GPO Customer Agencies, Contractors, and PII Liability

GPO informed us they are not liable for contract associated privacy data breach incidents. According to GPO's Customer Services Regional Operations Chief, GPO does not receive or process the customer's PII. Instead, customers are responsible for identifying, maintaining, and transferring their PII directly to the contractors. GPO's Customer Services Contracting Officers, in coordination with the customer, approve the contractor's security and PII handling plans, which are subsequently stored in the GPO contract files. When a privacy incident occurs, the breach is reported via the GPO 4049 Privacy Incident Reporting Form. The GPO employees, BU manager, BU PPOC, or Contracting Officers work with the customer and the contractor to identify

potential remedies, and may issue a cure notice to the contractor to address the issue. However, the contractor bears the liability for any potential damages or costs associated with privacy data breaches.

GPO has an obligation to safeguard PII and implement procedures for the handling of privacy data breach incidents as described in numerous federal statutes, regulations, and directives. Its process to receive and respond to reported incidents should minimize the impact of privacy data breaches, the risk of compromising customer data, and the risk of unauthorized use.

The GPO Incident Response Plan Documents Can Be Improved

PII breaches are hazardous to both individuals and organizations. Individual harms may include identity theft, embarrassment, or blackmail and significant financial losses. Organizational harm may include a loss of public trust, legal liability, and/or remediation costs. The harm PII breaches pose can be contained and minimized through the development of effective incident response plans to handle breaches involving PII. Effective incident response plans include elements such as determining when and how individuals should be notified, how a breach should be reported, and whether to provide remediation services to affected individuals.

NIST Special Publication 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, one of the references in the Privacy Program directive, states that organizations should develop an incident response plan to handle breaches involving PII. The plans should include elements such as determining when and how individuals should be notified, how a breach should be reported, and whether to provide remedial services, such as credit monitoring, to affected individuals.

The Privacy Program directive states that the GPO Privacy Officer is required to implement an Incident Response Plan. The Incident Response Plan consists of two documents:

- **PIRT Framework and Procedures**, a document that is focused on incident response procedures and internal/external protocols for notification of privacy breaches, and includes notification procedures for the GPO Inspector General, GPO CSIRT, and US-CERT.
- **PIHG**, a document distributed to the BU contacts, which defines BU obligations to protect PII, procedures describing how BU's must respond to the potential loss or compromise of PII, and the required protocols for reporting any breaches or compromises of PII to the GPO PIRT.

PIRT Framework and Procedures

The GPO incident handling procedures and guidance can be improved. The PIRT Framework and Procedures has an overall process but lacks detail. It does not have

specific incident response procedures that state how to perform an action. For example, it does not succinctly and clearly identify the specific duties for members of the PIRT. Nor does the PIRT Framework and Procedures have an incident response decision tree to lead the PIRT through the incident. Also, while the PIRT Framework and Procedures references communicating privacy breaches internally and externally, it does not have clear procedures on how to do so. For example, there is no statement of how communication should occur, such as through email or phone calls, and there are no templates of what information to share in the internal and external notifications. Finally, although the PIRT Framework and Procedures references notifying the OIG, GPO CSIRT, and US-CERT, it does instruct how to do it. For example, contact information such as phone numbers, email addresses, and website addresses are not documented in the PIRT Framework and Procedures. Clear PIRT Framework and Procedures instructions and guidance, including templates, would support more effective execution of a PIRT member's duties.

Privacy Incident Handling Guidance

The GPO PIHG is organized into a Frequently Asked Questions format. While it provides information about the PIRT Framework and Procedures and the process the PIRT follows to address potential breaches, it does not clearly help the BU contacts perform their responsibilities. The PIHG defines the obligation to protect PII by stating that all GPO personnel, including employees, contractors, subcontractors, and temporary staff are responsible for reporting privacy incidents following procedures established by their BU director or managers or BU PPOC. Additionally, the PIHG states there are strict employment consequences for failing to protect PII, including reprimand, suspension, and/or removal. However, the PIHG does not define the procedures to respond to the loss or compromise of PII. Additionally, the PIHG does not clearly identify how to report a privacy incident. Further, the PIHG does not have clear protocols to report an incident to US-CERT. The PIHG states that the Chief Information Officer (CIO) and/or the Chief of the IT Security Division, the Chief Privacy Officer, or the CIO's PPOC shall report incidents to US-CERT. However, the PIHG does not state how this information is to be reported to US-CERT, such as through a phone call, email, or a website. Additionally, the PIHG does not state what information is to be provided to US-CERT, nor how to document that the information was reported to US-CERT.

Instructions to report a breach are included in both the PIRT Framework and Procedures and the PIHG, although they are not aligned with each other. The PIRT Framework and Procedures specifically states that any suspected or confirmed PII incidents are to be reported using the Privacy Incident Reporting procedures. This includes contacting the employee's BU manager or the BU PPOC, completing and emailing the Privacy Incident Reporting Form 4049, and providing a copy of that form to the BU manager or BU PPOC. If neither the BU manager nor the BU PPOC is available, the employee should call the Policy Officer.[23] The PIHG states to report privacy incidents following the procedures

[23] At present, the GPO Policy Officer and the GPO Privacy Officer is a dual role, held by one person.

established by their BU director or managers or PPOC. This process means that there is no one, central method for reporting suspected breaches. GPO would benefit from a centralized and unified method to report suspected incidents.

Finally, remediation services are not mentioned in the PIRT, but offering credit monitoring is mentioned in the PIHG. However, the PIHG does not identify what levels of suspected or confirmed breaches are necessary to prompt the offering of credit monitoring services. The PIHG also does not identify the responsible party for monitoring services. Without robust guidance in the PIRT Framework and Procedures and the PIHG, GPO risks failing to adequately evaluate and respond to suspected PII breaches.

Recommendation 8. Update the PIRT Framework and Procedures to incorporate the guidance for incident response plans from NIST Special Publication 800-122 and include comprehensive guidance, such as:

a) defining team member roles and responsibilities
b) defining key terms
c) developing communication templates
d) ensuring notification of the appropriate individuals and organizations by identifying points of contact, including external entities, and how to contact them.

Management Comments

GPO concurred with this recommendation. While GPO believes that it currently meets much of this recommendation, as described below, it will review the published PIRT Framework and Procedures and assess how the items listed in Recommendation 8 can be further clarified and detailed.

Specifically, GPO stated that the appendices of the PIRT Framework and Procedures already address the recommendation in the following ways:

a. Appendix B of the PIRT document includes matrices showing PIRT incident handling teams, BUs involved, members in each team, and roles and responsibilities.
b. Appendix A of the PIRT document includes a list with a description of all acronyms used in the document. As suggested by this recommendation, GPO will update Appendix A to include the vocabulary of all terms used in the PIRT.
c. Appendix C of the PIRT document includes an incident form and actions required, however, as suggested by this recommendation, GPO will expand Appendix C to further detail the communication templates.
d. Appendices B and C of the PIRT document include notification of the appropriate individuals and organizations. However, GPO will update PIRT to include a detailed list of points of contact, including external entities, and their contact information.

OIG Response

GPO's concurrence and planned actions to further clarify and detail the recommended items are responsive to this recommendation.

We acknowledge that the PIRT Framework and Procedures includes "Appendix 1: Acronyms," a matrix of privacy incident teams, and a page titled "Incident Reporting Form." However, these sections of the PIRT Framework and Procedures do not define team member roles and responsibilities, define key terms, provide communication templates, and do not identify points of contact, including external entities, and how to contact them.

In order to close this recommendation, the agency must provide the updated PIRT Framework and Procedures that incorporates incident response plans from NIST Special Publication 800-122 and comprehensive guidance identified in the recommendation.

Recommendation 9. Update the PIHG to incorporate the guidance for incident response plans from NIST Special Publication 800-122 including comprehensive guidance, such as:

a) ensuring the proper notification of the appropriate individuals and organizations when evaluating and responding to a suspected PII breach, by identifying points of contact, including external entities, and how to contact them
b) stating what information is to be provided to US-CERT and the reporting method, such as through a phone call, email, or a website
c) stating how to document that the information was reported to US-CERT.

Management Comments

GPO concurred with this recommendation. GPO stated it will review and update the PIHG as necessary.

OIG Response

GPO's concurrence and planned actions are responsive to this recommendation. In order to close this recommendation, the agency must provide the updated PIHG that incorporates incident response plans from NIST Special Publication 800-122 and comprehensive guidance identified in the recommendation.

Recommendation 10. Develop and/or identify the one definitive method to report suspected PII breach incidents.

Management Comments

GPO concurred with this recommendation. GPO plans to utilize GPO's IT Service Hub, which is the IT Service Management System, to document the PII Incident Reporting and

Tracking. GPO expects this process will provide a consistent method of reporting suspected PII breach incidents.

OIG Response

GPO's concurrence and planned actions are responsive to this recommendation. In order to close this recommendation, the agency must provide evidence of the definitive method to report suspected PII breach incidents.

Finding 4: GPO should ensure that all employees receive PII training.

Over the period of this report, GPO did not provide privacy awareness training to all employees and contractors. GPO's Privacy Program directive requires each BU to ensure that individuals who could access, use, or disclose PII on GPO information systems receive appropriate training before being granted access. Additionally, the Privacy Officer is required to maintain the training program for employees having access to or managing PII. Any employee, regardless of their occupation, could be exposed to PII. Therefore, we assess, and benchmarking supports, that all employees should receive PII training. Further, we recommend that PII training be centralized under a single BU, likely Information Technology, to ensure employees and contractors receive PII training before accessing GPO's information systems.

Criteria

- OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*, January 3, 2017
- NIST Special Publication 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, April 2010
- GPO Directive 705.28B, *Information Technology Systems Development Life Cycle Policy*, October 22, 2019
- GPO Directive 825.33C, *Information Technology (IT) Security Program Statement of Policy*, March 19, 2021
- GPO Directive 825.41B *Privacy Program: Protective of Personally Identifiable Information (PII)*, April 06, 2021
- GPO Privacy Incident Handling Guidance (PIHG) Version 5, June 10, 2020
- GPO Privacy Incident Response Team (PIRT) Framework and Procedures Version 6, April 24, 2020

GPO Did Not Provide Privacy Awareness Training to All Employees and Contractors

GPO Privacy Program directive requires that employees having access to or managing PII are trained every 2 years. PII training is the responsibility of the Privacy Officer and the BUs. The Privacy Officer is responsible for maintaining GPO PII training and accomplishes this with the assistance of the Workforce Development, Education, and Training division. BUs are responsible for ensuring that all individuals in the BU receive appropriate training before being granted access to GPO information systems. Employees and contractors are responsible for collecting only the required, authorized PII; avoiding unauthorized disclosure or misuse of PII; and reporting known or suspected use of PII, including by contractors or subcontractors of procured contracts. GPO Directive 705.28B states that the CIO is responsible for the overall management of IT resources.[24] OMB

[24] GPO Directive 705.28B, *Information Technology Systems Development Life Cycle Policy*, October 22, 2019.

directs that agencies should consider annual security and privacy training as the baseline, with specialized training for specific groups.[25]

The GPO Privacy Officer created three forms of GPO privacy training for BU PPOCs.

1. *GPO Privacy Program Annual Privacy Briefing: Safeguarding Personally Identifiable Information (PII) (Training for GPO Privacy Point of Contacts)*, directed to BU PPOCs with a focus on internal privacy concerning employees and contractors working for GPO. The Privacy Officer calls this the BU Training.
2. *GPO Privacy Program Annual Privacy Briefing: Personal Health Privacy and Security Training Session (Training for GPO Human Capital Office/Medical Unit Privacy Point of Contacts)*, directed to Medical Unit PPOCs with a focus on internal privacy including PHI. The Privacy Officer calls this the PHI training.
3. *GPO Privacy Program Executive Briefing*, directed to GPO executives with an emphasis on awareness and best practices. Due to the Coronavirus Disease impacting the operating status and in-person restrictions, the Privacy Officer did not conduct this training.

Because any employee, regardless of their occupation, could be exposed to PII, all employees should receive PII training. For example, an employee could find documents with PII left in a breakroom, and would need to be able to identify the information as PII, know how to handle that PII, and report the incident appropriately.[26]

The BUs are responsible for training non-PPOC employees before granting them access to the GPO information systems. During our fieldwork, we did not request or review any of the training that BUs provide to non-PPOC employees, primarily because the initial focus was regarding the Privacy Officer's responsibilities, versus BU responsibilities. It was not readily apparent that the BU training responsibilities fell under the management and implementation of the Privacy Program. Subsequently, the GPO Director testified to Congress that GPO's Privacy Program applies to employees and contractors alike and affirmed the responsibility of everyone to promptly report potential privacy incidents and breaches. Therefore, training for all employees falls within the purview of the implementation of the Privacy Program.[27]

Additionally, the Privacy Officer could not provide evidence that contractors received PII training nor that they were provided copies of the Privacy Program directive. For example, in one of the requests for bid reviewed, a Security Control Plan was to be included as part of the bid for the contract, as part of the General Terms and Conditions of the contract. The contractor was to comply with security requirements specific to the

---

[25] OMB M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*, January 3, 2017

[26] While the Information Technology BU's Annual GPO IT Security Awareness Training references the Privacy Program directive, we assess that the three PII related bullets do not meet the spirit of this finding to ensure that all employees and contractors know how to recognize and protect PII, promptly report potential incidents, and understand the consequences of failing to safeguard PII.

[27] "Big Data: Privacy Risks and Needed Reforms in the Public and Private Sectors" Testimony before the Committee on House Administration, February 16, 2022.

agency for which the work would be completed. As the work could include exposure to PII information, the contractor was to ensure all staff completed security training from the specific agency. Further, immediately upon discovering any breach or suspected breach of security, the contractor was to notify the Contracting Officer's Representative. However, there was no mention of GPO's Privacy Program. Without ensuring contractors either receive training or are provided a copy of the Privacy Program directive, the Privacy Officer cannot ensure contractors are aware of their responsibility to protect PII or to report known or suspected breaches.

The Privacy Program directive does not clearly state how the Privacy Officer is to maintain the PII training program, nor that the training program includes the training required by BUs. Further, while the directive does not specifically task the Privacy Officer with a responsibility to ensure contractors receive PII training, the overall responsibility and authority for devising and implementing protective measures reside with the Privacy Officer. As such, the Privacy Officer should also maintain a program for contractors with access to or managing PII.

In comparison, as a best practice, the Departments of State (State) and Homeland Security (DHS) both require annual PII training. At State, the annual *Cyber Security Awareness* course contains a privacy awareness section. They also have a biennial *Protecting Personally Identifiable Information (PII)* course and advanced specialized privacy training for employees with PII intense activities. At DHS, privacy awareness is encouraged as part of the onboarding process, including when and how to report a privacy incident. DHS also has a mandatory annual refresher training, *Privacy at DHS: Protecting Personal Information.* For contractors whose solicitations and contracts include special clauses regarding safeguarding sensitive information and privacy training, DHS hosts a website with a myriad of security policies, privacy safeguards, and training.

As shown, in other agencies all employees are required to be trained on PII annually. Without training, staff may not know how to safeguard the information they are privy to. Employees may not know when or how to report unauthorized or other inadvertent misuses; and could be unaware of the potential penalties for doing so, including termination of employment and, for contractors, termination of a contract. The Privacy Officer should take into consideration best practices from other agencies, such as State and DHS, and ensure GPO has a comprehensive GPO PII training program, for both employees and contractors in addition to the PPOCs.

Further, the CIO is responsible for the overall management of IT resources and the IT Security Program.[28] The IT Security Program ensures adequate protection for all information and IT systems that collect, store, and share information, which includes systems with PII. Adequate protection includes securing the GPO information systems from unauthorized access and inappropriate information disclosure. Although GPO Directive 825.41B states that BUs are required to provide their staff with appropriate

[28] GPO Directive 825.33C, *Information Technology (IT) Security Program Statement of Policy*, March 19, 2021.

training before granting access to the GPO information systems, our analysis is that this responsibility would be better situated with the CIO. As the overall manager of IT resources, the CIO is ultimately responsible for safeguarding IT information systems and ensuring that anyone who accesses the IT information resources has appropriate permissions and training. GPO should implement a centralized training method under a single BU, likely Information Technology, to ensure employees and contractors receive PII training before accessing GPO's information systems.

Recommendation 11. Develop and implement a PII training program to ensure all GPO personnel, including employees, contractors, subcontractors, and temporary staff, are trained on PII roles and responsibilities, including applicable penalties for failing to protect PII. This training program should include:

a) Annual PII training in accordance with OMB Memorandum M-17-12;
b) PII and related records management training as part of the New Employee Orientation; and
c) Best practices from other agencies.

Management Comments

GPO concurred with this recommendation. While GPO believes that it currently meets much of this recommendation, it will ensure BU PPOCs complete training before accessing the information system and paper records containing PII. GPO will also ensure all employees and contractors who do not directly handle PII will be required to take the Privacy Basics training. GPO provided Human Capital with a pamphlet covering GPO Records Management and PII, which is to be shared with new employees. Finally, GPO will revisit its process of researching privacy programs implemented at various government agencies to identify opportunities for strengthening the GPO Privacy Program and the PII training conducted at GPO.

Specifically, GPO stated that the PII training program addresses the recommendation in the following ways:

a. GPO already instituted a comprehensive, specialized PII training program for all employees and contractors who handle PII as part of their daily job duties, as stated in GPO Directive 825.41B, Section 9.d.6 – Privacy Office Activities, which directs:

> "Maintain the training program for employees having access to or managing PII with the assistance of the Director of Workforce Development, Education, and Training. Inform each PPOC of the availability of PII Training. Maintain a log showing the PPOC PII training completion status. PII training must be taken once every two years."

This specialized training is offered through GPO's Workforce, Development, Education, and Training Learning Management System. All employees and contractors who handle PII are required to complete this training once every two years. Since August 2020, approximately 220 GPO employees and contractors

identified by their BU management completed this training. GPO asserted that BUs, in collaboration with the Privacy Office, have already assumed the responsibility of this specialized PII training. GPO stated BUs will further ensure that BU PPOCs who have a need to access systems and databases containing PII complete this training before receiving permission to access the information system and paper records containing PII.

GPO stated that in addition, all GPO employees and contractors who do not directly handle PII will be required to take the Privacy Basics training. This training, PII Awareness & Best Practices, is available on GPO's intranet. The Privacy Office will collaborate with GPO's Workforce, Development, Education, and Training to start announcing this as mandatory training and make it available through their training portal.

b. GPO provided Human Capital with a pamphlet covering GPO Records Management and Personally Identifiable Information to be shared with new employees.

c. GPO researched privacy programs implemented at various Government agencies, such as State, DHS, and many others while developing Directive 825.41B. However, GPO will revisit this process to identify opportunities for strengthening the GPO Privacy Program, Directive 825.41B, and the PII training conducted at GPO.

OIG Response

GPO's concurrence and planned actions to ensure all GPO employees and contractors take Privacy training, and to revisit best practices from other agencies are responsive to this recommendation.

We acknowledge that GPO has various privacy training, which were identified earlier in our report. However, GPO only requires that employees having access to or managing PII take training once every two years, instead of annually, which would be in accordance with OMB Memorandum M-17-12.

We reviewed the PII Awareness & Best Practices training, which is intended for GPO employees and contractors who do not directly handle PII. While the document provides a broad overview of PII and references GPO Directive 825.41B, *Privacy Program: Protection of Personally Identifiable Information (PII)*, we assess that the training lacks key elements required for a comprehensive understanding of an individual's roles and responsibilities. For example, the training does not include potential consequences of not protecting PII, such as identity theft. Nor does the training cover potential consequences or disciplinary actions for the GPO employees. In addition, the training omits examples of how employees could encounter PII, such as finding a printed emergency contact list that includes an employee's name, home address, and personal phone number(s), or other sensitive documents, such as a Standard Form 52. Finally, the training does not

incorporate an employee's obligation to protect and report suspected PII breaches, which the GPO Director emphasized as a fundamental principle of GPO's Privacy Program.[29]

We acknowledge that GPO views providing a pamphlet about Records Management and PII as sufficient to address this portion of the recommendation to consider new employees trained on PII roles and responsibilities, including the applicable penalties for failing to protect PII. However, this information should also be provided verbally during New Employee Orientation.

We reiterate that GPO's PII training program should ensure all GPO personnel, including employees, contractors, subcontractors, and temporary staff, are trained on PII roles and responsibilities, including the applicable penalties for failing to protect PII. This training program should include annual training, training as part of New Employee Orientation, and best practices from other agencies.

In order to close this recommendation, the agency must provide a comprehensive PII training program document, identifying how all GPO personnel are and will be trained on PII roles and responsibilities, the associated training materials, and the frequency of that training. The agency must also identify which best practices it reviewed from other agencies, and its reasoning for adopting or not adopting that best practice.

Recommendation 12. Implement a central training method to ensure employees and contractors receive PII training before accessing GPO's information system. This method should include reassigning the responsibility for annual training to a single BU, likely Information Technology, and assigning BUs with the responsibility for specialized PII training.

Management Comments

GPO concurred with this recommendation.

OIG Response

GPO's concurrence is responsive to this recommendation. In order to close this recommendation, the agency must provide evidence of a central training method that ensures employees and contractors receive PII training before accessing GPO's information systems.

Recommendation 13. Update the Privacy Program directive to reflect changes resulting from these recommendations.

[29] "Big Data: Privacy Risks and Needed Reforms in the Public and Private Sectors" Testimony before the Committee on House Administration, February 16, 2022.

Management Comments

GPO concurred with this recommendation. GPO will update Directive 825.41B as necessary.

OIG Response

GPO's concurrence and planned action is responsive to this recommendation. In order to close this recommendation, the agency must provide the updated Privacy Program directive to reflect the changes resulting from these recommendations. Additionally, the agency must update all other associated directives, policies, procedures, guidance, and training to reflect applicable changes to the Privacy Program directive.

Appendix A. Table of Recommendations

Recommendation	Management Response	Status	Return on Investment
Director			
1. Identify the federal privacy laws and oversight guidance, and their applicable sections, that GPO intends to follow as definitive guidance. Include the reasoning and/or basis for those determinations.	GPO will revisit other OMB and NIST guidance and standards and evaluate how GPO can further strengthen its Privacy Program.	Open	Monetary – Cost avoidance *Agencies and individuals can be penalized $5,000 for each Privacy Act violation.* Nonmonetary – Improve management controls, avoid adverse publicity, provide analysis/data to decision-makers *Identifying the specific sections of laws and guidance GPO follows, and documenting the reasoning for following some sections but not others will help guide GPO's future decision-making and privacy practices. It will ensure proper controls are in place in appropriate systems, and it will ensure appropriate parties have been advised of GPO's practices.*
2. Develop PIAs for the five untracked PII systems identified: HC Dashboard, APEC ABTC, DC One Card ID, Pentagon Contractors ID Card, and TWIC®.	GPO will develop PIAs for the HC Dashboard, APEC ABTC, DC One Card ID, Pentagon Contractors ID Card, and TWIC®.	Open	Monetary – Cost avoidance *Creating PIAs for the untracked PII systems will help ensure that GPO avoids data breaches, which cost an average of $4.4 million each in 2022.* Nonmonetary – Improve management controls, improve systems/processes *Creating PIAs for the untracked PII systems will help ensure that proper safety measures, processes, and controls are in place.*
3. Identify the mechanism to document confidentiality impact levels and document the confidentiality impact levels for all GPO PII systems.	GPO will establish the confidentiality impact level for each system and update each PIA to reflect the confidentiality impact level.	Open	Monetary – Cost avoidance *Documenting confidentiality impact levels to help determine the appropriate safeguards to apply to PII*

Recommendation	Management Response	Status	Return on Investment
			will help ensure that GPO avoids data breaches, which cost an average of $4.4 million each in 2022. Nonmonetary - Improve management controls, improve systems/processes *Documenting confidentiality impact levels will help GPO determine appropriate safeguards to apply to PII.*
4. Implement a process to conduct BU PII inventories and share the results with the Privacy Officer	GPO's plans to survey each BU to inventory PII captured by the BU in September 2022	Open	Monetary – Cost avoidance *Conducting BU PII inventories, and sharing the results with the Privacy Officer, will help GPO identify the inventory of PII records that need to be protected from a data breach. A data breach cost an average of $4.4 million in 2022.* Nonmonetary - Improve management controls, improve systems/processes *Ensuring that both GPO and its BUs have a full accounting of the PII systems in use will allow GPO to ensure controls and processes are in place to protect PII.*
5. Conduct biennial Privacy Compliance Reviews in accordance with GPO's Privacy Program directive.	GPO plans to commence biennial PCR in August 2022.	Open	Monetary – Cost avoidance *Conducting Privacy Compliance Reviews will help GPO ensure protections for PII records are appropriate and sufficient to protect that information from a breach. A data breach cost an average of $4.4 million in 2022.* Nonmonetary - Improve management controls, improve systems/processes *Ensuring the PCRs are completed will ensure any changes to the PII system are documented and the*

Recommendation	Management Response	Status	Return on Investment
			appropriate controls and processes to protect the PII are in place.
6. Review all stored records to identify and mark which records contain or may contain PII.	GPO plans to inspect and mark all hard copy boxes in Records Management's possession to reflect the presence of PII. GPO will also update the revised database to reflect the presence of PII in records.	Open	Monetary – Cost avoidance *Identifying and labeling which records contain PII will help GPO be able to quickly identify if the records were impacted in the event of a breach. A data breach cost an average of $4.4 million in 2022.* Nonmonetary - Improve management controls, improve systems/processes, initiate best business practices *Identifying and marking all records that contain PII will allow the appropriate controls and processes to be applied to protect the PII. Being able to quickly and easily identify the sensitivity of any material is a best business practice.*
7. Update the Records Management Program directive and the corresponding GPO Form 1350 to clearly state that records transferred to Records Administration & Management Division, for storage and destruction, must indicate whether or not the records contain PII.	GPO will approve and publish the revised GPO Directive 840.1B, Records Management Program, and GPO Form 1350, Records Transmittal and Receipt. The updated form will include the capability to mark the presence of PII in the records being transferred.	Open	Monetary – Cost avoidance *Updating directives and forms to identify which records contain PII will help GPO be able to quickly identify if the records were impacted in the event of a breach. A data breach cost an average of $4.4 million in 2022.* Nonmonetary - Improve management controls, improve systems/processes, initiate best business practices *An updated directive and form can describe how GPO will ensure it identifies the appropriate controls and processes are applied to protect sensitive material. Labeling the sensitivity of*

Recommendation	Management Response	Status	Return on Investment
			any material is a best business practice.
8. Update the PIRT Framework and Procedures to incorporate the guidance for incident response plans from NIST Special Publication 800-122 and include comprehensive guidance, such as: a) defining team member roles and responsibilities b) defining key terms c) developing communication templates d) ensuring notification of the appropriate individuals and organizations by identifying points of contact, including external entities, and how to contact them.	GPO will review the published PIRT Framework and Procedures and assess how the items listed in Recommendation 8 can be further clarified and detailed.	Open	Nonmonetary - Improve management controls, improve systems/processes, initiate best business practices, validate existing processes *Updating guidance to clearly define roles and responsibilities, define key terms, include communication templates, and ensure appropriate notification will allow GPO to ensure PII incidents are responded to in a manner that remediates the incident in a timely and thorough manner. Updating the guidance will also allow GPO to validate if a new employee could follow and implement the guidance without additional information.*
9. Update the PIHG to incorporate the guidance for incident response plans from NIST Special Publication 800-122 including comprehensive guidance, such as: a) ensuring the proper notification of the appropriate individuals and organizations when evaluating and responding to a suspected PII breach, by identifying points of contact, including external entities, and how to contact them b) stating what information is to be provided to US-CERT and the reporting method, such as through a phone call, email, or a website c) stating how to document that the information was reported to US-CERT.	GPO will review and update the PIHG as necessary.	Open	Nonmonetary - Improve management controls, improve systems/processes, initiate best business practices, validate existing processes *Updating guidance to ensure proper notification of others as well as clarifying what information is to be provided and how to document that notification happened will allow GPO to ensure PII incidents are responded to in a manner that remediates the incident in a timely and thorough manner. Updating the guidance will also allow GPO to validate if a new employee could follow and implement the guidance without additional information.*
10. Develop and/or identify the one definitive method to report suspected PII breach incidents.	GPO plans to utilize GPO's IT Service Hub, the IT Service Management System, to document the PII Incident	Open	Nonmonetary - Improve management controls, improve systems/processes

Recommendation	Management Response	Status	Return on Investment
	Reporting and Tracking. GPO expects this process will provide a consistent method of reporting suspected PII breach incidents.		*Using one definitive method to report suspected PII breach incidents will allow GPO to ensure consistency with the information reported. It will allow the reported incident to reach the appropriate responders in a timely manner.*
11. Develop and implement a PII training program to ensure all GPO personnel, including employees, contractors, subcontractors, and temporary staff, are trained on PII roles and responsibilities, including applicable penalties for failing to protect PII. This training program should include: a) Annual PII training in accordance with OMB Memorandum M-17-12; b) PII and related records management training as part of the New Employee Orientation; and c) Best practices from other agencies.	GPO states it will ensure PU PPOCs complete training before accessing the information system and paper records containing PII. GPO will also ensure all GPO employees and contractors who do not directly handle PII will be required to take the Privacy Basics training. GPO states they already provided Human Capital with a pamphlet covering GPO Records Management and PII, which is to be shared with new employees. Finally, GPO states it will revisit its process of researching privacy programs implemented at various government agencies to identify opportunities for strengthening the GPO Privacy Program and the PII training conducted at GPO.	Open	Monetary – Cost avoidance *Providing PII training to all employees on their PII roles and responsibilities will help GPO avoid a PII breach. A data breach cost an average of $4.4 million in 2022.* *Agencies and individuals can be penalized $5,000 for each Privacy Act violation.* Nonmonetary - Improve management controls, improve systems/processes, initiate best business practices, improve security, avoid adverse publicity *Ensuring all GPO employees, contractors, subcontractors, and temporary staff are trained on PII roles and responsibilities will help keep PII safe and secure.*
12. Implement a central training method to ensure employees and contractors receive PII training before accessing GPO's information system. This method should include reassigning the responsibility for annual training to a single BU, likely Information Technology, and assigning BUs with the responsibility for specialized PII training.	GPO plans to address this recommendation.	Open	Nonmonetary - Improve management controls, improve systems/processes, initiate best business practices, improve security, avoid adverse publicity *A centralized training method will ensure employees and contractors receive PII training before accessing GPO's information system. This centralized training method is a control to ensure only trained staff potentially access PII; improves the safety of PII systems by ensuring GPO staff can identify PII, including if it*

Recommendation	Management Response	Status	Return on Investment
			is misplaced; and matches best business practices used by other agencies.
13. Update the Privacy Program directive to reflect changes resulting from these recommendations.	GPO states it will update Directive 825.41B as necessary.	Open	Monetary – Cost avoidance *Providing an updated directive with clear roles and responsibilities will help GPO avoid PII data breaches. A data breach cost an average of $4.4 million in 2022.* *Agencies and individuals can be penalized $5,000 for each Privacy Act violation.* Nonmonetary - Improve management controls, improve systems/processes, initiate best business practices, improve security *Updating the Privacy Program directive to reflect changes implemented due to these recommendations will ensure the most accurate information is provided to GPO employees and contractors.*

Appendix B. Scope and Methodology

Scope

The organizational scope of this inspection included the GPO Privacy Officer and BUs that collect, store, process and dispose of PII, and the members of the PIRT.

Methodology

The inspection team:

- Interviewed:
    - The GPO Privacy Officer
    - Senior managers responsible for the implementation of the GPO Privacy Program directive, within:
        - Customer Services,
        - Human Capital,
        - Security & Intelligent Documents,
        - the Superintendent of Documents, and
        - Records Administration & Management Division
    - BU staff that handle PII, as defined by their procedures.
- Performed walkthroughs of the Records Administration & Management Division storage rooms, the Security & Intelligent Documents Return Book Processing Center, and the Secure Card Production System card waste processing center.
- Reviewed a sample of contracts identified as processing PII for GPO in the Customer Services division.
- Reviewed policies and procedures associated with the Privacy Program.

This inspection was conducted in accordance with the *Quality Standards for Inspections and Evaluations of the Council of the Inspectors General on Integrity and Efficiency*, January 2012 (Blue Book). Note: This inspection began before the updated 2020 Blue Book implementation was required, so it was completed in accordance with the 2012 procedures.

Appendix C. Abbreviations

ABTC	APEC Business Travel Card
APEC	U.S. Asia-Pacific Economic Cooperation
BU	Business Unit
CIO	Chief Information Officer
CSIRT	Computer Security Incident Response Team
DC	District of Columbia
DHS	Department of Homeland Security
DOB	Date of Birth
FDsys	Federal Digital System
GPO	U.S. Government Publishing Office
ID	Identification Card
IT	Information Technology
NIST	National Institute of Standards and Technology
OGC	Office of General Counsel
OIG	Office of the Inspector General
OMB	Office of Management and Budget
OPM	Office of Personnel Management
PCR	Privacy Compliance Review
PHI	Protected Health Information
PIA	Privacy Impact Assessment
PIHG	GPO Privacy Incident Handling Guidance
PII	Personally Identifiable Information
PIRT	Privacy Incident Response Team
PPOC	Privacy Point of Contact
Privacy Act	*The Privacy Act of 1974*, as amended, 5 U.S.C. Section 552a
PTA	Privacy Threshold Analysis
SDA	System Disposal Assessment
SORN	System of Records Notice
State	Department of State
SSN	Social Security Numbers
TWIC®	Transportation Worker Identification Credential
U.S.C.	United States Code
US-CERT	United States Computer Emergency Readiness Team

Appendix D. Management Comments

HUGH NATHANIAL HALPERN
Director

GPO

MEMORANDUM

Subject: Response to OIG Draft Report – Privacy Program Inspection, Project Number 21-01-II

Date: July 12, 2022

To: Inspector General

This memorandum responds to the IG Draft Report – Privacy Program Inspection, Project Number 21-01-II.

GPO appreciates the draft report's recognition of the progress made in several areas of the GPO Privacy Program. We concur with many of the report's findings in that the Agency needs to improve in a number of areas to strengthen its Privacy Program. Currently, GPO has one employee in the Privacy Office, however, we are in the process of hiring a Junior Privacy Officer to assist the Privacy Office expedite progress on the reported recommendations.

Recommendation 1

Identify the federal privacy laws and oversight guidance, and their applicable sections, that GPO intends to follow as definitive guidance. Include the reasoning and/or basis for those determinations.

GPO concurs with this recommendation.

In establishing GPO's Privacy Program, GPO researched Federal laws and guidance available from the Office of Management and Budget (OMB), National Institute of Standards and Technology (NIST), and National Archives and Records Administration (NARA). We also studied privacy programs of various Government agencies.

We performed this research with the goal of including the laws and guidance that demonstrated practices to best implement for a robust privacy program at GPO. The following laws and guidance best applied to the scope and activities referenced in GPO Directive 825.41B, Privacy Program: Protection of Personally Identifiable Information (PII):

- Privacy Act of 1974, as amended, 5 U.S.C. § 552a. Although not applicable to GPO, the Privacy Act outlines Fair Information Practice Principles.
- OMB Memorandum M-16-14, dated July 1, 2016, discusses the use of Government-wide blanket purchase agreements (BPAs) for Identity Monitoring, Data Breach Response, and Protection Services.
- OMB Memorandum M-17-06, Policies for Federal Agency Public Websites and Digital Services, dated November 8, 2016, states, "The agency's Privacy Program

Page must be located at www.[agency].gov/privacy and must be accessible through the agency's "About" page."

- OMB Memorandum M-17-12, dated January 3, 2017, provides guidance regarding preparing for and responding to a breach of Personally Identifiable Information.
- NIST Special Publication 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) (Final), dated April 6, 2010.

In accordance with this recommendation, GPO will revisit other OMB and NIST guidance and standards and evaluate how GPO can further strengthen its Privacy Program.

GPO anticipates completion of this recommendation by December 30, 2022.

Recommendation 2

Develop PIAs for the five untracked PII systems identified: HC Dashboard, APEC ABTC, DC One Card ID, Pentagon Contractors ID Card, and TWIC®.

GPO concurs with this recommendation.

GPO will develop Privacy Impact Assessments (PIAs) for the following five systems:

- Human Capital (HC) Dashboard;
- U.S. Asia-Pacific Economic Cooperation (APEC) Business Travel Card (ABTC);
- District of Columbia (DC) One Card ID;
- Pentagon Contractors ID Card; and
- Transportation Worker Identification Credential (TWIC®).

GPO anticipates completion of this recommendation by December 30, 2022.

Recommendation 3

Identify the mechanism to document confidentiality impact levels and document the confidentiality impact levels for all GPO PII systems.

GPO concurs with this recommendation.

Finding 3 of the draft report states, "GPO's privacy incident response procedures should incorporate NIST Special Publication 800-122 in order to provide more detailed implementation guidance when responding to privacy incidents and breaches."

GPO's current Privacy Incident Response Team (PIRT) Framework and Procedures actually refer to NIST eight times. In addition, the mechanism suggested in this recommendation for documenting confidentiality impact levels is illustrated in Section 3 of the PIRT Guide. However, GPO will update the PIRT Guide, as necessary, to further elaborate on applicable guidelines included in NIST Special Publication 800-122.

GPO will also collaborate with Business Unit (BU) Managers to update the inventory of PII for each of the 19 GPO systems carrying PII. Once the GPO PII inventory is updated, GPO will conduct the PIRT documented process to establish the confidentiality impact level for each system and update each PIA to reflect the confidentiality impact level.

GPO anticipates completion of this recommendation by November 30, 2022.

Recommendation 4

Implement a process to conduct BU PII inventories and share the results with the Privacy Officer.

GPO concurs with this recommendation.

As stated in GPO Directive 825.41B, Section 9.e – Business Unit's PII Activities, GPO surveys each BU to inventory PII captured by the BU. The next survey is scheduled for September 2022. The Privacy Office distributes a spreadsheet with instructions to the BUs for submitting the PII used in the BU and for submitting any plans the BU has to curtail the use of PII. GPO shared an account of all BU PII Holdings as part of the OIG PO Inspection Data Call Documents with staff name (IG's Office) through SharePoint on March 3, 2021.

GPO anticipates completion of this recommendation by October 31, 2022.

Recommendation 5

Conduct biennial Privacy Compliance Reviews in accordance with GPO's Privacy Program directive.

GPO concurs with this recommendation.

GPO plans to commence biennial Privacy Compliance Reviews (PCRs) in August 2022. GPO is hiring a Junior Privacy Officer who, once on-board, will assist the Privacy Officer with these compliance reviews.

GPO anticipates completion of the Privacy Compliance Reviews by February 2023.

Recommendation 6

Review all stored records to identify and mark which records contain or may contain PII.

GPO concurs with this recommendation.

GPO's Privacy Office is collaborating with the Records Management unit to develop a process for inspecting and marking existing records that may contain PII. The Privacy team will take additional steps to modify the current database for capturing metadata regarding PII. Further, the Privacy Office, in collaboration with Records Management and the BUs, will inspect all hard copy boxes in Records Management's possession and mark them to reflect the presence of PII. GPO will also update the revised database to reflect the presence of PII in records.

GPO expects to complete this action item by November 30, 2022.

In addition to inspecting and marking existing records, GPO is preparing a Statement of Work (SOW) to acquire and implement an Electronic Records Management (ERM) system to facilitate inventorying, housing, and management of GPO records. The metadata captured for GPO records will facilitate PII tracking, management, and redaction as required.

GPO plans to complete this action item by February 2023.

Recommendation 7

Update the Records Management Program directive and the corresponding GPO Form 1350 to clearly state that records transferred to Records Administration & Management Division, for storage and destruction, must indicate whether or not the records contain PII.

GPO concurs with this recommendation.

GPO recently revised GPO Directive 840.1B, Records Management Program, and GPO Form 1350, Records Transmittal and Receipt. The updated form includes the capability to mark the presence of PII in the records being transferred.

GPO anticipates the approval and publishing of the updated Directive and form by August 31, 2022.

Recommendation 8

Update the PIRT Framework and Procedures to incorporate the guidance for incident response plans from NIST Special Publication 800-122 and include comprehensive guidance, such as:

a. *defining team member roles and responsibilities*
b. *defining key terms*
c. *developing communication templates*
d. *ensuring notification of the appropriate individuals and organizations by identifying points of contact, including external entities, and how to contact them*

GPO concurs with this recommendation.

a. Appendix B of the PIRT document includes matrices showing PIRT incident handling teams, BUs involved, members in each team, and roles and responsibilities.
b. Appendix A of the PIRT document includes a list with a description of all acronyms used in the document. As suggested by this recommendation, GPO will update Appendix A to include the vocabulary of all terms used in the PIRT.
c. Appendix C of the PIRT document includes an incident form and actions required, however, as suggested by this recommendation, GPO will expand Appendix C to further detail the communication templates.
d. Appendices B and C of the PIRT document include notification of the appropriate individuals and organizations. However, GPO will update PIRT to include a detailed list of points of contact, including external entities, and their contact information.

In summary, while the Agency believes that it currently meets much of this recommendation, GPO will review the published PIRT Framework and Procedures and assess how the items listed in Recommendation 8 can be further clarified and detailed.

GPO anticipates completion of this recommendation by December 31, 2022.

Recommendation 9

Update the PIHG to incorporate the guidance for incident response plans from NIST Special Publication 800-122 including comprehensive guidance, such as:

a. *ensuring the proper notification of the appropriate individuals and organizations when evaluating and responding to a suspected PII breach, by identifying points of contact, including external entities, and how to contact them*
b. *stating what information is to be provided to US-CERT and the reporting method, such as a through a phone call, email, or a website*
c. *stating how to document that the information was reported to US-CERT*

GPO concurs with this recommendation.

GPO will review and update the GPO Privacy Incident Handling Guidance (PIHG) as necessary.

GPO anticipates completion of this recommendation by December 31, 2022.

Recommendation 10

Develop and/or identify the one definitive method to report suspected PII breach incidents.

GPO concurs with this recommendation.

GPO plans to utilize GPO's IT Service Hub, which is the IT Service Management System (ITSM), to document the PII Incident Reporting and Tracking. This process will provide a consistent method of reporting suspected PII breach incidents.

GPO anticipates completion of this task by December 30, 2022.

Recommendation 11

Develop and implement a PII training program to ensure all GPO personnel, including employees, contractors, subcontractors, and temporary staff, are trained on PII roles and responsibilities, including applicable penalties for failing to protect PII. This training program should include:

a. *Annual PII training in accordance with OMB Memorandum M-17-12;*
b. *PII and related records management training as part of the New Employee Orientation; and*
c. *Best practices from other agencies.*

GPO concurs with this recommendation.

a. GPO already instituted a comprehensive, specialized PII training program for all employees and contractors who handle PII as part of their daily job duties.

   As stated in GPO Directive 825.41B, Section 9.d.6 – Privacy Office Activities: "Maintain the training program for employees having access to or managing PII with the assistance of the Director of Workforce Development, Education, and Training. Inform each PPOC of the availability of PII Training. Maintain a log showing the PPOC PII training completion status. PII training must be taken once every two years."

This specialized training is offered through GPO's Workforce, Development, Education, and Training (WDET) Learning Management System (LMS). All employees and contractors who handle PII are required to complete this training once every two years. Access to the PIRT Framework and Procedures document and GPO Directive 825.41B is provided as part of this training. A quiz with a passing score is required to complete the training. WDET provides a comprehensive report listing the names and emails of all employees and contractors scheduled to take this training along with a completion status. Since August 2020, approximately 220 GPO employees and contractors identified by their BUs' management completed this training. Therefore, BUs in collaboration with the Privacy Office have already assumed the responsibility of this specialized PII training. BUs will further ensure that BU Privacy Points of Contact (PPOCs) who have a need to access systems and databases containing PII complete this training before receiving permission to access the information system and paper records containing PII.

In addition, all GPO employees and contractors who do not directly handle PII will be required to take the Privacy Basics training. GPO already developed and published this training (PII Awareness & Best Practices) which is available on GPO's intranet. The Privacy Office will collaborate with GPO's WDET to start announcing this as a mandatory training and make it available through the WDET training portal. Access to GPO Directive 825.41B is incorporated in this training.

b. GPO provided Human Capital with a pamphlet covering GPO Records Management and Personally Identifiable Information to be shared with new employees.

c. While developing Directive 825.41B, GPO researched privacy programs implemented at various Government agencies, such as the Department of State, Department of Homeland Security (DHS), and many others. However, GPO will revisit this process to identify opportunities for strengthening the GPO Privacy Program, Directive 825.41B, and the PII training conducted at GPO.

Recommendation 12

Implement a central training method to ensure employees and contractors receive PII training before accessing GPO's information system. This method should include reassigning the responsibility for annual training to a single BU, likely Information Technology, and assigning BUs with the responsibility for specialized PII training.

GPO concurs with this recommendation and anticipates completion of this task by October 31, 2022.

Recommendation 13

Update the Privacy Program directive to reflect changes resulting from these recommendations.

GPO concurs with this recommendation.

GPO will update Directive 825.41B as necessary. GPO anticipates completion of this task by February 2023.

Thank you for the opportunity to respond. The Agency spent approximately 45 hours preparing the response to this request. If you have further questions about this matter, please contact me

Digitally signed by Hugh N Halpern
Date: 2022.07.12 12:30:38 -04'00'

HUGH NATHANIAL HALPERN
Director, U.S. Government Publishing Office

cc:
Deputy Director

[Back *Cover Placeholder*]