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 Dan Rose (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