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

SEPTEMBER 2024

U.S. Government Publishing Office

Audit Report: Management of Excess and Obsolete Paper and Secure Documents

OIG Report Number 24-08


U.S. GOVERNMENT PUBLISHING OFFICE
710

Questions, Copies, Suggestions

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

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

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

Fax: 202-512-1352

Email: gpoighotline@gpo.gov

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

U.S. GOVERNMENT PUBLISHING OFFICE

OIG

OFFICE *of the* INSPECTOR GENERAL

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

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

MEMORANDUM
OIG-24-064

Date: September 18, 2024

To: Director, U.S. Government Publishing Office

From: Inspector General, U.S. Government Publishing Office

Subject: Audit Report: Management of Excess and Obsolete Paper and Secure Documents, Report Number 24-08

The U.S. Government Publishing Office, Office of the Inspector General conducted an audit of the Management of Excess and Obsolete Paper and Secure Documents, Project Number A-2024-001.

We reported two findings and three recommendations to improve the management of defective blank U.S. Passport books and provisions in an interagency agreement. Management agreed with the findings and recommendations. We made no substantive changes to the final report from the draft based on Management's comments. However please note that on page 6, we deleted a reference to the June 2019 security assessment report (SAR) because we did not review the said SAR. We identified this error after the exit meeting but inadvertently left it in the formal draft report issued. The difference is as follows:

- Draft Report: "We've reviewed GPO's June 2019 and July 2023 SARs, and the contractor's FY 2023 penetration testing results…"
- Final Report: "We've reviewed GPO's July 2023 SAR and the contractor's FY 2023 penetration testing results…"

We include a summary and analysis of Management's comments on page 10, and they are included in their entirety in Appendix D. The planned corrective actions should resolve the issues identified in the report.

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

NATHAN J. DEAHL
Inspector General

RESULTS IN BRIEF

What We Did

The Office of the Inspector General conducted an audit of the U.S. Government Publishing Office's (GPO) management of excess and obsolete paper and secure documents. Our objective was to determine if management uses effective processes to account for, store, and destroy secure intelligent documents and products. Our audit focused on U.S. passport production.

GPO is responsible for producing blank U.S. passport books for the Department of State (DoS), with whom they maintain a Memorandum of Understanding (MOU). There are various provisions in the MOU that GPO must follow relating to security and product integrity, from acquiring raw materials from suppliers through the storage, production, and destruction process to shipping finished blank U.S. passport books to DoS.

GPO reported over 54.9 million books were produced for DoS in fiscal years (FY) 2021 through 2023. For the same period, almost 2.4 million books were rejected during production and DoS returned 80,456 books. Any U.S. passport books deemed defective by GPO and DoS must be collected, analyzed, validated, and destroyed under a controlled environment.

What We Recommend

We made three recommendations to address the secure storage of defective U.S. passport books, inventory control system reviews, and security protocol training.

What We Found

Finding 1. GPO was responsible for securely storing and destroying over 2.4 million defective U.S. passport books in FYs 2021 through 2023. GPO has two different procedures for storing defective U.S. passport books. Books rejected during production are placed in bins without locks on the production floor. In contrast, books returned from DoS are stored in a dedicated locked room that can be accessed only by designated employees. We also found that areas where employees perform on-site shredding of defective U.S. passport books were not monitored by security cameras.

These conditions occurred, in part, because management 1) relied on security cameras in production areas as a control that allowed them to leave rejected U.S. passport books in bins without locks and 2) did not install security cameras in shredder areas. We acknowledge the presence of security cameras can provide a deterrent. However, we believe that management can further increase controls by storing all defective U.S. passport books in a locked space where accountability can be assigned. Regarding missing security cameras, based on our audit, management took immediate action to install security cameras in shredder areas.

Finding 2. Management could strengthen its compliance with MOU provisions to maintain a passport inventory control system that complies with federal information security requirements and ensure employees take DoS-approved security protocol training. According to management, GPO's internal security assessment reviews and privacy training met the applicable MOU provisions. We believe that taking additional steps to align GPO actions with applicable MOU provisions could help reduce the risk of data breaches and provide increased confidence in the U.S. passport production data used to inform management decisions and financial reporting. Also, it could provide reasonable assurance that employees are handling U.S. passport books in accordance with GPO and DoS security protocols.

TABLE OF CONTENTS


PASSPORT
United States of America

INTRODUCTION

Objective

This report presents the results of our self-initiated audit of the Management of Excess and Obsolete Paper and Secure Documents (Project Number A-2024-01). Our objective was to determine if management uses effective processes to account for, store, and destroy secure intelligent documents and products. Our audit focused on U.S. passport production. In April 2024, our office initiated an investigation significant to our audit objective. As of this report date, the investigation is ongoing. Consequently, in accordance with Government Auditing Standards,[1] we suspended work on the applicable portion of the engagement and completed the remaining portions of the engagement. We will continue to monitor the investigation and may follow up with a future audit. See Appendix A for additional information about the objective, scope, and methodology of this audit.

Background

GPO is a legislative branch agency responsible for the production and distribution of information products for all three branches of the Government. This includes official publications of Congress, the White House, and other Federal agencies, and the courts.

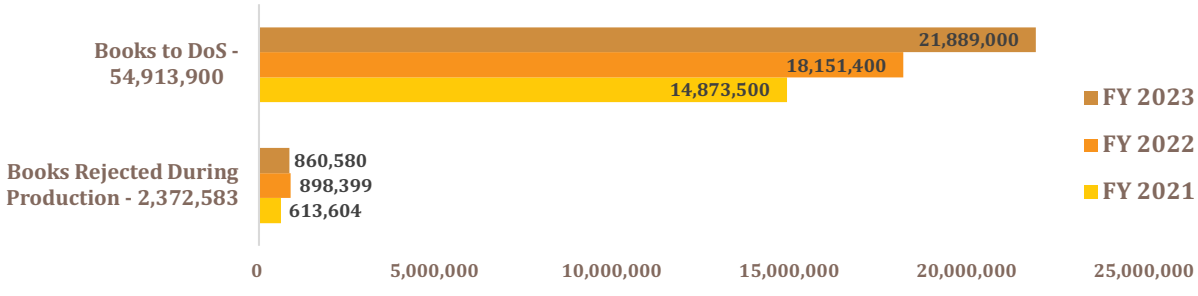
For nearly a century, GPO has been responsible for producing the U.S. passport for the U.S. Department of State. For decades, the U.S. passport was a conventionally printed document. Beginning in 2005, the U.S. passport incorporated a digital chip and other enhanced security features capable of carrying biometric identification data. According to GPO, the U.S. passport that it produces in Washington, D.C., as well as at a secure remote facility in Mississippi, is considered the most secure identification credential.

In May 2023, GPO renewed its Memorandum of Understanding (MOU) with the U.S. Department of State (DoS), Bureau of Consular Affairs Passport Services Directorate. The prior MOU became effective in November 2009. The MOU established that GPO is responsible for the security and product integrity of U.S. passport production, from acquiring raw materials from suppliers through the storage, production, and destruction process to shipping finished blank U.S. passports to DoS. Among other administrative duties and functions, the MOU also set forth provisions for inventory control system reviews and security protocol training. To carry out its functions, GPO contracts with a supplier to provide technical support and software license maintenance for U.S. passport production.

[1] Government Auditing Standards §8.27, Investigations and Legal Proceedings, requires auditors to evaluate the effect of in-process investigation proceedings on the current audit.

Within GPO, the Security and Intelligent Documents Business Unit (SID) is responsible for the production of blank U.S. passport books. As shown in Figure 1, GPO reported that they produced over 54.9 million books for DoS and rejected almost 2.4 million books during production in FYs 2021 through 2023. While the MOU did not establish a waste rate, GPO collects spoilage and production waste information for its annual production cost review with DoS.

Figure 1. Number of U.S. Passport Books Produced by Fiscal Year



Source: GPO Reports.

In addition, GPO reported that DoS returned a total of 80,456 books in FYs 2021 through 2023. Subsequently, GPO and DoS agreed that 12,445 of the total returned books were due to DoS errors. Therefore, GPO and DoS considered 68,011 returned books as post-production defective books for errors such as wrinkled pages or visible glue spots. The MOU established the maximum annual GPO defect rate threshold to be 0.5 percent for U.S. passport books shipped to DoS. For FYs 2021 through 2023, GPO's post-production defect rate ranged from 0.04 percent to 0.18 percent, well below the established defect rate threshold of 0.5 percent. Any U.S. passport books deemed defective by GPO and DoS must be collected, analyzed, validated, and destroyed under a controlled environment, as shown in Figure 2.

Figure 2: Defective U.S. Passport Destruction Process

Source: GPO Procedure Documents.

AUDIT RESULTS

Finding 1. Secure Storage and Destruction of Defective U.S. Passport Books

While GPO management ensures SID operates in secure facilities, we found that management could improve security controls related to defective U.S. passport books. During our site visits at both SID facilities from January through May 2024, we observed unsecured storage of defective U.S. passport books and inadequate security camera coverage of shredder areas.

According to the MOU, GPO must securely store and destroy any U.S. passport production waste due to the sensitive nature of the materials and security features in blank U.S. passport books, including raw materials and blank books. From FY 2021 through 2023, almost 2.4 million were rejected during production due to quality issues. In addition, DoS returned over 80,000 U.S. passport books during the same period. Therefore, GPO was responsible for securely storing and destroying over 2.4 million U.S. passport books in FYs 2021 through 2023.

Rejects from Production
2,372,583 U.S passport books

Returns from DoS
80,456 U.S. passport books

Storage of Defective U.S. Passport Books

SID has two procedures for storing defective U.S. passport books. For blank U.S. passport books rejected during production, employees at both SID facilities collect and place books in bins without locks on the production floor until they are destroyed. In contrast, employees store all DoS returned U.S. passport books in a dedicated room in the Washington, D.C. facility. This dedicated room can be accessed from a keyless padlock because some of the returned books contain personally identifiable information (PII) of American citizens. SID employees analyze and validate all defective U.S. passport books before any books can be destroyed. See Figure 3 for the two storage and destruction procedures.

Figure 3: Storage and Destruction of Defective U.S. Passport Books

According to SID management, they use security cameras as a control that allows them to leave blank U.S. passport books in a bin without locks on the production floor. We spoke with GPO Security management, and they confirmed that hundreds of security cameras are installed throughout the two SID facilities. During each work shift at both SID facilities, there is one security officer monitoring rotating camera feeds on multiple screens in a control room. We acknowledge that the presence of security cameras can provide a deterrent. However, we believe that management can further increase controls by storing all defective books in a locked space where accountability can be assigned. By ensuring that all defective books are secured prior to destruction, there is a reduced risk of missing or lost books going undetected.

Security Camera Coverage

We found that at both SID facilities, the areas where SID employees perform on-site shredding of defective U.S. passport books were not monitored by security cameras. In April 2024, we informed GPO Security management of the missing security cameras. They explained that they installed security cameras to monitor nearby doors, not specifically to view the shredder areas. However, GPO Security management agreed that said areas should have dedicated security cameras to monitor shredding activities. GPO Security management also acknowledged that they should have identified the missing security cameras during their annual security assessments of GPO facilities.

In May 2024, we informed GPO Security management that the cameras they installed in the shedder areas were not recording properly. They agreed and adjusted camera settings to continuously monitor the shredder areas at both SID facilities. In June 2024, we observed the installed security cameras addressed the issue identified in this audit. Consequently, we will not make any recommendations for this issue at this time.

Recommendations for the Director, GPO:

Recommendation 1: Develop procedures to securely store all defective U.S. passport books until they are destroyed.

Finding 2. Memorandum of Understanding Compliance

GPO management could strengthen its compliance with provisions related to the passport inventory control system and security protocol training. Specifically, section V.C., *Inventory Control System*, of the MOU requires that GPO collect and maintain U.S. passport production information in a database system that is Federal Information Security Modernization Act[2] (FISMA) compliant. Further, section IV.I., *Security Protocol for PII*, requires that GPO employees with access to PII take the annual *Passport Data Security Awareness* course offered by DoS or an equivalent course approved by DoS.

FISMA[3] Compliant Database System

As part of our audit, we reviewed applicable provisions of the MOU significant to our audit objective. The MOU requires GPO to maintain a FISMA-compliant database system to hold all passport production data. According to the interagency agreement, GPO must follow their jointly developed inventory control protocol on the use of chips to track passport production information such as:

> *"…chip acquisition information, chip failures, chip serial numbers, correlation of chip serial numbers to passport numbers, and any related information necessary to oversee the production, inventory control, failure rate of procured chips, and controls of passport shipped…"*

What is FISMA compliance?

An essential framework for ensuring the security of government information and systems. It involves risk assessments, security controls, monitoring, and independent annual reviews.

To meet its MOU obligations, GPO contracted with a supplier to provide a comprehensive production management solution. Under the contract, the supplier licenses its proprietary software to GPO and provides on-site technical support at both SID facilities. GPO refers to the supplier's proprietary software as the ePassport Application. The ePassport Application tracks U.S. passport production from start to finish as prescribed in the MOU, section V.C., *Inventory Control System*. Also, the ePassport Application interfaces detailed passport production data with GPO's main database system.

We held joint and separate discussions with senior SID and Information Technology Business Unit (IT) officials about the Agency's FISMA compliance per applicable MOU provisions.[4] During a follow-up discussion on April 25, 2024, management stated that they were aware of the FISMA requirements in the MOU. They added that GPO continually strived to be FISMA compliant for the ePassport Application. For example, management performed periodic tests for known exploited vulnerabilities. Also, management contracted with a supplier to perform annual penetration testing. Further, management stated that they plan to strengthen its test model by performing security testing and assessments each year.

[2] The MOU referenced the Federal Information Security Management Act of 2002. However, the Federal Information Security Modernization Act of 2014, Pub. L. 113–283 amended the Federal Information Security Management Act of 2002, Pub. L. 107–347, Title III (codified in Title 44, Chapter 35).

[3] FISMA's definition of "agency" does not include GPO.

[4] The requirement for a FISMA-compliant electronic inventory system was included in both the November 2009 and May 2023 MOUs with DoS.

Management added that due to costs, a decision was made several years ago to not use an independent reviewer. Instead, management increased GPO IT resources to conduct and issue security assessment reports (SAR) to support the Authority to Operate (ATO) for the ePassport Application. We've reviewed GPO's July 2023 SAR and the contractor's FY 2023 penetration testing results and found some key FISMA requirements related to assessing and monitoring controls were not included. The SARs showed "In Place" for over 200 security controls. We also found GPO policies[5] require an internal security assessment of its system to be performed every three years instead of an annual independent review.

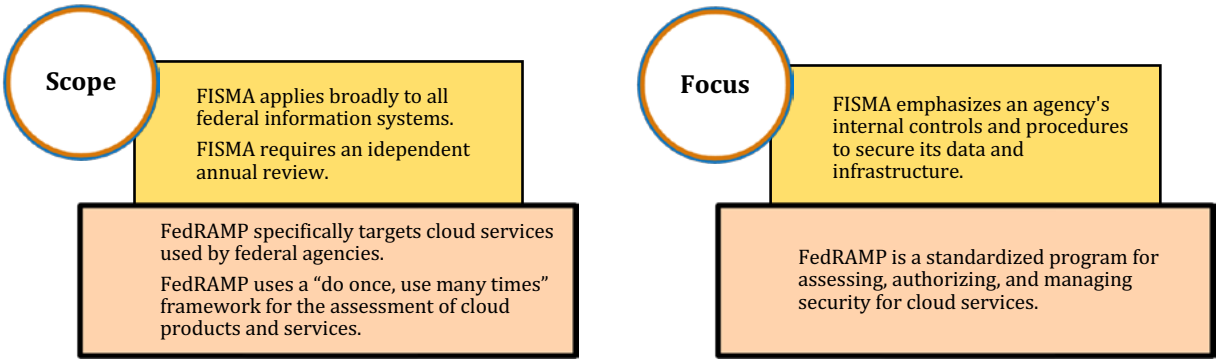
What is an ATO?

ATO is the process through which GPO assesses the risk of operating a particular IT system and decides whether to accept that risk.

In subsequent discussions, management stated that GPO's main database system is the official inventory system for U.S. passport production, not the ePassport Application. Management asserted that since GPO's main database system resides on a secure cloud application, and that the cloud application is FedRAMP[6] certified, GPO would not need any additional FISMA compliance for its main database system.

Congress enacted FISMA in 2002. It was amended in 2014 to strengthen and protect federal agency information and their information systems. FISMA provides a complete framework to ensure the effectiveness of security controls over information resources that support federal operations and assets. We recognize that FISMA's definition of "agency" does not include GPO.[7] However, because GPO and DoS entered into a MOU that establishes the obligations of each in support of U.S. passport production, and DoS falls within the scope of FISMA, we believe that GPO has voluntarily agreed to maintain a FISMA-compliant database system. Absent documentation that demonstrates the cloud application service provider that supports GPO's main database system is FISMA compliant, we believe being FedRAMP certified is not a substitution (see Figure 4 for key differences). Also, GPO's internal security assessment is not an independent validation of FISMA compliance that offers objectivity and regulatory adherence.

Figure 4. Key Differences Between FISMA and FedRAMP



[5] Directive 825.33C, *Information Technology (IT) Security Program Statement of Policy*.

[6] FedRAMP, Federal Risk and Authorization Management Program, is a security program for cloud service providers seeking to do business with the federal government.

[7] 44 U.S.C. §§ 3502(1); 3552(a).

We also recognize that both GPO's main database system and the ePassport Application store historical data related to U.S. passport production. However, the ePassport Application, a supplier's propriety software, is the entry point into GPO's main database system for all U.S. passport production data that informs management of sensitive and timely decisions. Therefore, taking additional steps to improve compliance with applicable MOU provisions or ensure MOU provisions align with GPO actions could help protect GPO's interest in a program that generated annual revenue of $495 million and $341 million in FY 2023 and FY 2022, respectively. Also, maintaining a FISMA-compliant database system can help reduce the risk of data breaches and provide increased confidence in the U.S. passport production data used to inform management decisions and financial reporting.

Security Protocol Training

The MOU, section IV.I., *Security Protocol for PII*, requires GPO personnel with access to PII to take the annual DoS *Passport Data Security Awareness* course or an equivalent course approved by DoS. This specific training requirement was added when the MOU was renewed in May 2023.

We inquired about attendance records for the DoS *Passport Data Security Awareness* course with SID management. Upon review, SID management informed us that they had elected to not require designated SID employees to take the DoS course because it is based on DoS systems and controls, which would not be relevant to GPO employees. However, SID management did not seek a waiver to the DoS course or obtain approval to substitute it with GPO's privacy training.

According to SID management, 18 employees handle U.S. passports with American citizen PII in them and all 18 employees have completed the annual GPO privacy training. We reviewed the GPO privacy training materials and found that while the GPO training covers PII handling, it is not specific to handling U.S. passports with PII and passport data sharing. See Table 1 for passport data privacy requirements.

Table 1. MOU Passport Data Privacy Requirements

Responsibilities to Protect Passport Privacy	Included in GPO Privacy Training
GPO employees will be advised of rules governing the handling of PII data on U.S. citizens covered under the Privacy Act.[8]	✓
Any unauthorized activity (unauthorized or accidental access, use, dissemination, disclosure, storage, or disposal of PII in passports) involving PII contained in defective passports by GPO personnel is to be reported promptly to appropriate officials in GPO as well as in DoS.	X
GPO acknowledges its requirement to report any suspected or confirmed data breach involving PII contained in defective passports to DoS.	X
GPO will investigate in the event of suspicious unauthorized activity related to PII contained in defective passports and will assist DoS with an examination of unauthorized activity related to such information.	X
GPO will report the result of any investigation of unauthorized activity related to PII contained in defective passports, including disciplinary action GPO has taken to hold responsible GPO personnel who committed an unauthorized activity, to DoS.	X

Source: GPO-DoS MOU, Appendix B, and GPO Privacy Training materials.
Key: ✓ = included X = not included

Based on our audit, SID management took immediate action and sent the GPO privacy training to DoS for approval. As of this report date, SID management had not yet received approval to substitute the DoS *Passport Data Security Awareness* course.

Ensuring designated employees take the DoS-approved training could provide reasonable assurance that employees are handling U.S. passport books in accordance with GPO and DoS security protocols specific to protecting the PII of American citizens and reporting potential breaches to DoS.

Recommendations for the Director, GPO:

Recommendation 2: Obtain Federal Information Security Modernization Act compliance for the passport production database system or work with the Department of State to reassess if the Memorandum of Understanding, section V.C., provisions should be amended.

Recommendation 3: Ensure designated employees take the Department of State *Passport Data Security Awareness* course or obtain approval to substitute said training with an equivalent course.

[8] While GPO is not required to comply with the Privacy Act of 1974, they have established the GPO Privacy Program by incorporating Federal regulations as best practices and other GPO policies that provide direction and guidance concerning security planning.

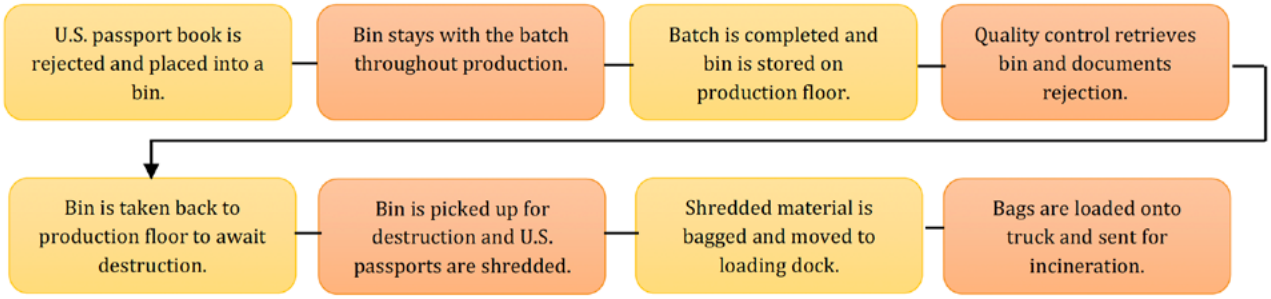
Other Matters of Interest

As a result of the ongoing investigation, referenced earlier in this report, we suspended work on the applicable portion of the engagement. However, we identified two areas that warrant management consideration for action - the standardization of procedures and U.S. passport book shredding.

First, the policies and procedures that we've reviewed for both SID facilities showed different ways of handling sensitive materials. For example, the Washington, D.C., facility requires that all documentation relating to the shredding of U.S. passport books be maintained for two years and that shredding information be recorded in a hard-copy destruction log. In contrast, the Mississippi facility does not specify a period for document retention. The Mississippi facility also does not maintain a hard-copy destruction log but instead requires their employees to update a spreadsheet database once a batch is reconciled.

Second, during our site visits at both SID facilities, we observed that U.S. passport book destruction is performed by a single employee. As described in the procedures below, for both facilities the same employee confirms the count of books to be destroyed is accurate, shreds the books, and returns the bin to the production floor. We believe that two employees should be present for the shredding of defective U.S. passport books to verify that the correct number of books are destroyed to reduce the risk impact for lost or missing books.

Figure 5: U.S. Passport Destruction Process



Source: GPO Procedure Documents.

We recognize that management has flexibility in how they establish and implement the U.S. passport production program. However, it is important for GPO to strike the right balance between autonomy and standardization when the same product is produced and destroyed at different locations. Opportunities to increase efficiency and reduce the risk that missing or lost books go undetected could be realized by standardizing destruction processes at both SID facilities.

Considerations for the Director, GPO:

Consideration 1: Standardize U.S. passport book destruction processes across SID facilities.

Consideration 2: Assign two employees to be present for the shredding of U.S. passport books to verify that the correct number of books are destroyed.

MANAGEMENT'S COMMENTS

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

Regarding recommendation 1, management stated that they will revise standard operating procedures (SOP) and Work Instructions to include major factors to ensure the secure storage of all defective passport books and the associated work-in-process before destruction. The target implementation date (TID) is November 30, 2024.

Regarding recommendation 2, management stated that they will work with the DoS to reassess and edit, as needed, the current DoS/GPO MOU. Management added that they will ensure that the applicable text in the MOU accurately describes GPO's current passport database system as FedRAMP and FISMA-certified. The TID is September 30, 2025.

Regarding recommendation 3, management stated that they have recently combined certain relevant elements from the DoS *Passport Data Security Awareness* training course with the existing GPO PII training course to create a new equivalent course. SID has requested approval from DoS to substitute said training with a GPO equivalent course. All SID employees will be required to take this course annually. The GPO Privacy Office will own and hold this coursework, administer the testing for all SID employees, and manage and maintain the testing results and history. The TID is February 1, 2025.

EVALUATION OF MANAGEMENT'S COMMENTS

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

APPENDICES

Appendix A. Objective, Scope, and Methodology

Our objective was to determine if the process GPO uses is effective to account for, store, and destroy secure intelligent documents and products. In April 2024, our office initiated an investigation with significant overlap to our audit objective. Consequently, we suspended work on the applicable portion of the engagement and completed the remaining portions of the engagement. As of this report date, the investigation is ongoing. We will continue to monitor the investigation and may follow up with a future audit.

To accomplish our objective, we:

- Reviewed applicable GPO and SID procedures and work instructions related to U.S. passport production, security, and destruction.
- Reviewed the MOU between GPO and the DoS for U.S. passport production, including relevant appendices and supporting documents.
- Reviewed documentation from FYs 2021 through 2023, including destruction logs, shipping manifests, waste processing reports, financial system records and reports, and employee training records.
- Reviewed security camera footage of U.S. passport shredder areas.
- Conducted walkthroughs to evaluate processes and procedures that GPO officials used to account for, store, and destroy U.S. passport books.
- Held discussions with applicable key personnel involved with the management of U.S. passport production, storage, security, and destruction.
- Interviewed GPO IT officials to gain an understanding of how GPO secures its electronic U.S. passport inventory system, including FISMA compliance.
- Traveled with SID personnel to observe the destruction of secure U.S. passport waste at a commercial incineration facility.

To determine how GPO accounted for U.S. passport and paper waste, we met with GPO Finance personnel to determine how they account for and record paper and U.S. passport waste in the financial statements. We also reviewed U.S. passport cost information from FYs 2021 through 2023 to determine how the waste was reflected in the cost.

To determine how GPO stored U.S. passports and paper waste, we had walkthroughs of the production floors in both the Washington, D.C. and Mississippi facilities. During the walkthroughs, we noted how both completed and waste of U.S. passport books were stored throughout the production and destruction processes.

To determine how GPO securely destroyed U.S. passport waste, we had walkthroughs of the destruction process and observed U.S. passport books being destroyed. We also observed U.S. passport waste being transported offsite and incinerated. We also reviewed security camera coverage of the U.S. passport shredder areas at both facilities.

We assessed GPO's compliance with two provisions in the MOU with DoS – FISMA compliant database system and security protocol training. To assess FISMA compliance, we obtained documentation from GPO IT officials and interviewed those officials. To determine if GPO followed the training requirement, we reviewed the training records of staff in the SID Returned Book Processing Center and interviewed SID management.

We conducted this performance audit from February 2024 through September 2024, in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. We discussed our observations and conclusions with management on August 15, 2024, and included their comments where appropriate.

Computer-Generated Data

We assessed the reliability of GPO's passport production inventory system by interviewing knowledgeable officials to obtain an understanding of controls and by conducting walkthroughs of processes relevant to our audit objective. We determined that the data were sufficiently reliable for the purposes of this report.

Internal Controls

We assessed internal controls and compliance with laws and regulations necessary to satisfy audit objectives.

Prior Audit Coverage

The OIG did not identify any prior audits, inspections, or investigations related to the objective of the audit within the last five years.

Appendix B. Table of Recommendations

Recommendation	Management Response	Status	Return on Investment
Director, GPO			
1. Develop procedures to securely store all defective U.S. passport books until they are destroyed.	Concur. TID November 30, 2024.	Open	Nonmonetary – Improve systems and processes. By implementing this recommendation, GPO could reduce the risk of missing or lost books going undetected for potential fraud activities, such as counterfeit production.
2. Obtain Federal Information Security Modernization Act compliance for the passport production database system or work with the Department of State to reassess if the Memorandum of Understanding, section V.C., provisions should be amended.	Concur. TID September 30, 2025.	Open	Nonmonetary – Ensure compliance with a prescribed standard. By implementing this recommendation, GPO could reduce the risk of data breaches and improve security posture to enhance trust and operational efficiency.
3. Ensure designated employees take the Department of State Passport Data Security Awareness course or obtain approval to substitute said training with an equivalent course.	Concur. TID February 1, 2025.	Open	Nonmonetary – Ensure compliance with a prescribed standard. By implementing this recommendation, GPO can raise confidence that they provided the appropriate training on DoS security protocols that can help protect the integrity and reputation of the passport production program.

Appendix C. Abbreviations

ATO	Authority to Operate
DoS	Department of State
FedRAMP	Federal Risk and Authorization Management Program
FISMA	Federal Information Security Modernization Act
FY	Fiscal Year
GPO	Government Publishing Office
IT	Information Technology
MOU	Memorandum of Understanding
OIG	Office of Inspector General
PII	Personally Identifiable Information
SAR	Security Assessment Report
SID	Security and Intelligent Documents Business Unit
SOP	Standard Operating Procedure
TID	Target Implementation Date

Appendix D. Management's Comments

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

HUGH NATHANIAL HALPERN
Director

MEMORANDUM

Date: September 11, 2024

To: Inspector General

Subject: Agency Response to the Draft OIG Report on the Management of Excess and Obsolete Paper and Secure Documents.

Thank you for the opportunity to offer the Agency's response to the OIG Draft Report on the Management of Excess and Obsolete Paper and Secure Documents.

Agency Response to Recommendations in the Draft Report

Recommendation 1

Develop procedures to securely store all defective U.S. passport books until destroyed.

GPO concurs with this recommendation.

GPO will revise Standard Operating Procedures (SOP) and Work Instructions to include the major factors below to ensure the secure storage of all defective passport books and the associated work-in-process before destruction.

1. District of Columbia (DC): As batches on the production lines are finished, the waste's red totes will be taken directly to the secure room Quality Control (QC) lab in DC. Once waste processing has been completed, totes will be delivered to the Material and Transportation Division, which takes possession and conducts secure destruction. Books will be held in that group's locked cage.

2. Stennis Production Facility (SPF): As batches are finished on the production lines, the waste's red totes will be taken directly to a secure cage in the Disintegrator Room and locked. Badge access will be limited to the QC team and Bindery Supervisors. The secure cage must be built, and a badge reader must be installed in SPF.

3. The books in process on the production floor must be kept adjacent to the production equipment in accessible totes while the batches are running. Once the batches are completed, the above steps will occur.

4. The supervisor will lock the waste books in a rolling cage if a batch is not completed at the end of a shift with a time gap to the next shift. Each bindery supervisor will have a key to the cage and will be able to open it at the start of the next shift. A "master" key will be in the custody of the Production Manager.

The Agency expects to build the SPF secure cage, complete the SOP review, and implement necessary managerial and supervisory changes by November 30, 2024.

Recommendation 2

Obtain Federal Information Security Modernization Act (FISMA) compliance for the passport production database system or work with the Department of State to reassess if the Memorandum of Understanding, section V.C., provisions should be amended.

GPO concurs with this recommendation.

The GPO will work with the Department of State (DOS) to reassess the current DOS/GPO Memorandum of Understanding and ensure that the applicable text accurately describes the GPO's current passport database system as Federal Risk and Management Program (FedRAMP) and FISMA-certified.

The GPO successfully self-certifies that the entire passport production IT system is FISMA compliant during the regular Authority to Operate (ATO) audit process. The passport production database system is an integral part of the entire passport production IT system that is audited and granted an ATO by the GPO's Information Technology Chief Information Officer. The ATO covers the whole system, including its database, software, and equipment. This ATO encompasses various documents and activities, such as the System Security Plan, Risk Assessment Report, Contingency Plan, Privacy Impact Assessment, Vulnerability Assessment, Penetration Testing, and more. Additionally, GPO conducts weekly vulnerability scans on different system subnets and an annual penetration test using a third-party vendor to ensure compliance with FISMA's requirements. In addition to the passport database system being FedRAMP certified, GPO also conducts regular scans and tests throughout the year to ensure FISMA compliance.

We will work with the DOS to reassess and edit, as needed, the current DOS/GPO Memorandum of Understanding. The Agency expects to complete this work by September 30, 2025.

Recommendation 3

Ensure designated employees take the Department of State Passport Data Security Awareness course or obtain approval to substitute said training with an equivalent course.

GPO concurs with this recommendation.

The GPO has recently combined certain relevant elements from the DOS Passport Data Security Awareness training course with the existing GPO Personally Identifiable Information (PII) training course to create a new equivalent course. Upon review, the Department of State PII Passport Data Security Awareness coursework is very specific to their environment and needs. Most elements of this coursework do not apply to SID's role in the Passport Program. SID has provided this new equivalent course to the Department of State to obtain their approval as a substitute for the Passport Data Security Awareness course.

All SID employees will be required to take this course annually. The GPO Privacy Office will own and hold this coursework, administer the testing for all SID employees, and manage and maintain the testing results and history.

The Agency expects to complete the course review and implement this training by February 1, 2025.

Thank you for the opportunity to provide the Agency's input on this product from your office. The Agency spent approximately 16 hours preparing this response.

If you have any questions, please contact me.

HUGH NATHANIAL HALPERN

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

OFFICE *of the* INSPECTOR GENERAL

U.S. GOVERNMENT PUBLISHING OFFICE

America Informed

gpoighotline@gpo.gov