



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

SPRING 2026



SEMIANNUAL REPORT TO CONGRESS

October 1, 2025 – March 31, 2026



U.S. GOVERNMENT PUBLISHING OFFICE



This report is available on our web site:

<https://www.gpo.gov/who-we-are/our-agency/inspector-general/semiannual-reports-to-congress>

710



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

ABOUT THE GOVERNMENT PUBLISHING OFFICE

The U.S. Government Publishing Office (GPO) was established in 1861 and is the Federal Government's primary resource for producing, procuring, cataloging, indexing, authenticating, disseminating, and preserving the official information products of the U.S. Government in digital and tangible formats. GPO is responsible for producing and distributing informational products and services for all three branches of the Federal Government, including U.S. passports for the Department of State and official publications of Congress, the White House, and other Federal agencies. In addition to publication sales, GPO provides permanent public access to Federal Government information at no charge through GovInfo.gov and via partnerships with libraries nationwide participating in the Federal Depository Library Program.¹

ABOUT THE OFFICE OF THE INSPECTOR GENERAL

The GPO Office of the Inspector General (OIG) promotes economy, efficiency, and effectiveness in GPO operations. Our efforts are designed to prevent and detect fraud, waste, and abuse.

The GPO Inspector General Act of 1988, 44 U.S.C. §§ 3901-3903, along with the Inspector General Act of 1978, as amended (IG Act), establishes the OIG's responsibilities and duties. The Legislative Branch Inspectors General Independence Act of 2019 enhanced the OIG's independence. It expanded our office's duties by, among other things, granting us independent law enforcement authority, human capital, and budget independence.

The OIG, located in Washington, D.C., is allocated 24 employees and is organized into a Front Office, which includes the Counsel to the Inspector General, and three operational divisions: Audits, Inspections, and Investigations. We conduct independent and objective reviews of GPO programs and operations to assist in keeping the Director, Congress, and the public informed of potential issues or deficiencies.

¹ <https://www.gpo.gov/who-we-are/our-agency/mission-vision-and-values>



GPO OIG MISSION/VISION/VALUES

OUR MISSION

To conduct independent, objective, and trusted oversight that promotes positive change for GPO, Congress, and the public.

OUR VISION

Champion integrity and excellence.

OUR VALUES

► PROFESSIONALISM

Exhibit characteristics and qualities that contribute to a positive work environment.

► ETHICAL

Commitment to be morally sound, fair, and accountable.

► EFFECTIVENESS

Innovate, collaborate, produce, and deliver.

► HONESTY

Communicate transparently with our colleagues and our customers.

► INCLUSIVENESS

Foster a diverse, supportive, welcoming environment for our employees and customers.

► KINDNESS

Treat one another with respect.





A MESSAGE FROM THE INSPECTOR GENERAL



I am pleased to present the U.S. Government Publishing Office (GPO) Office of the Inspector General's Semiannual Report to Congress for the period October 1, 2025, through March 31, 2026. This report highlights the significant accomplishments of our Audits, Inspections, and Investigations Divisions as we continue our mission to promote integrity, efficiency, and accountability across GPO's programs and operations.

During this reporting period, our office advanced meaningful oversight through a combination of strategic audits, targeted inspections, and both reactive and proactive investigative work. We issued multiple reports identifying opportunities to strengthen management controls, improve cybersecurity maturity, enhance workforce processes, and reinforce program integrity. Across the organization, our findings and recommendations provide practical, data-driven pathways to greater efficiency, reduced risk, and more transparent operations.

Our audit work examined key areas including cybersecurity incident response, financial reporting, and follow-up on previously issued recommendations. Inspections addressed critical mission areas such as human capital, force protection, secure document production, and quality control processes. Investigators handled 93 intakes, closed 10 cases, and continued initiatives in cybersecurity contract performance. Each division's contributions reinforced the importance of collaboration, independence, and vigilance.

We also maintained a strong focus on transparency and accountability. All required reporting elements under the Inspector General Act are included, and we continued to monitor potential concerns such as whistleblower retaliation, senior official investigations, and agency interference—none of which were identified this period. Our office remains fully committed to upholding the standards established by the Council of the Inspectors General on Integrity and Efficiency.

As GPO continues to evolve in support of Congress and the American public, our office will remain steadfast in its oversight responsibilities. I am proud of the professionalism and dedication shown by every member of the OIG team. Together, we will continue advancing our mission of independent, objective, and trusted oversight that champions integrity and excellence.

A handwritten signature in black ink that reads "Nathan J. Deahl". The signature is written in a cursive, flowing style with a long horizontal line extending to the right.

Nathan J. Deahl
Inspector General



TABLE OF CONTENTS

ABOUT THE GOVERNMENT PUBLISHING OFFICE	I
ABOUT THE OFFICE OF THE INSPECTOR GENERAL	I
GPO OIG MISSION/VISION/VALUES	III
A MESSAGE FROM THE INSPECTOR GENERAL	V
TABLE OF CONTENTS	1
SELECTED STATISTICS AND HIGHLIGHTS	2
RETURN ON INVESTMENT	3
LIST OF NON-MONETARY BENEFITS	4
JOINT OIG PROJECTS	5
COMPLETED	5
AUDITS	6
ONGOING	6
COMPLETED	6
INSPECTIONS	8
ONGOING	8
COMPLETED	8
INVESTIGATIONS	9
CASE HIGHLIGHTS	10
OTHER INFORMATION	13
APPENDIX A. PEER REVIEW RESULTS	14
APPENDIX B. NON-MONETARY RETURN ON INVESTMENT	15
APPENDIX C. INVESTIGATIONS STATISTICS	18
APPENDIX D. OPEN OIG RECOMMENDATIONS	20
APPENDIX E. STATUS OF OIG RECOMMENDATIONS	23
APPENDIX F. REPORTING REQUIREMENTS	24
APPENDIX G. ABBREVIATIONS AND ACRONYMS	25
APPENDIX H. GLOSSARY OF TERMS	26

SELECTED STATISTICS AND HIGHLIGHTS

Audits

Reports Issued or Issued Under Audits' Oversight3

Inspections

Reports Issued or Issued Under Inspections' Oversight3

Investigations

Complaints Opened 28

Complaints Closed 19

Investigative Cases Opened 3

Investigative Cases Closed 10

Subpoenas Issued 0

Investigative Referrals to GPO Management4

Recommendations

Recommendations Opened 11

Recommendations Closed 16

RETURN ON INVESTMENT

Return on Investment (ROI) is a commonly used profitability ratio that measures the return or profit an investment generates relative to cost.² The ROI for an OIG is the most quantifiable performance metric, considering the cost of doing business and the revenues it collects.³ As amended, the reporting requirements of the Inspector General Act of 1978 prioritize quantitative results rather than qualitative work. Therefore, Inspectors General may focus on metrics that may not accurately reflect the most pressing matters at the agency they oversee.⁴ This can lead to misplaced emphasis in OIG's work because it focuses on money lost, whereas much of its value comes from money saved or, in other words, the value gained, *i.e.*, proactive savings as opposed to reactive losses.

For OIG work, ROI is usually defined in terms of monetary impact and savings associated with audits, investigations, and other actions that allow the government to recoup funds owed, correct practices to ensure more efficient spending, and prevent misappropriation of funds.⁵ The appendices to this report include examples of these types of monetary benefits; some cases are required by law to be reported.

While dollar value is the traditional baseline for ROI, there are other quantitative and qualitative ways to show a positive impact, such as expanding the definition of "value." Examples of ways to measure value can be savings over time, better decision-making and reporting, increased level of service, and timely regulatory compliance.⁶

Including this expanded concept of ROI in reporting to GPO, Congress, and the public is important. The results and impact of OIG work often provide an alternative to the traditional monetary ROI and give the flexibility to develop tailored approaches for determining agency operations' efficiency, effectiveness, or sustainability. Examples of non-monetary or non-traditional benefits are listed on the following page.

² Speights, "Return on Investment: What to Expect," *The Motley Fool* (March 17, 2021), available at: <https://www.fool.com/investing/how-to-invest/stocks/good-return-on-investment/>

³ Hudak and Wallack, "Sometimes cutting budgets raises deficits: The curious case of inspectors general return on investment," *Center for Effective Public Management at Brookings* (April 2015), available at: <https://www.brookings.edu/wp-content/uploads/2016/06/CEPMHudakWallackOIG.pdf>

⁴ Letter to Senator Johnson, Senator Peters, Representative Cummings, and Representative Jordan from ACORN8, Government Accountability Project, National Taxpayers Union, Project on Government Oversight, Public Citizen, R Street Institute, and Taxpayers Protection Alliance (May 16, 2019), available at: <https://www.rstreet.org/wp-content/uploads/2019/05/Bipartisan-Coalition-Support-Letter-for-IG-reform.pdf>

⁵ IBID.

⁶ "Calculating Non-Traditional Return on Investments," *VUEWorks* (Feb. 26, 2018), available at: <https://www.vueworks.com/calculating-non-traditional-return-on-investments/>

List of Non-Monetary Benefits

- 01)** Improve management controls
- 02)** Improve systems and processes
- 03)** Avoid violations of law or regulations
- 04)** Validate existing processes
- 05)** Initiate best business practices
- 06)** Provide analysis and data to decision-makers
- 07)** Improve safety, morale, health, and security
- 08)** Ensure compliance with a prescribed standard
- 09)** Enhance stakeholder confidence
- 10)** Other

We provide a narrative of each project's ROI in Appendix B.

JOINT OIG PROJECTS

In keeping with our strategic direction, OIG efforts will be “team-based.” In addition, we will use team members from each division to work on joint projects and products.

Completed

GPO Site Visits Follow-Up Inspection, Report No. 26-01, December 15, 2025

From May through June 2025, our office sent a joint team of investigators and inspectors to GPO’s two distribution centers and the Stennis Secure Production Facility (SPF) to evaluate any actions taken by GPO to address the considerations outlined in our May 2022 GPO OIG Regional Site Visit Report. We also sought to educate GPO employees on the OIG’s mission and their role in detecting fraud, waste, abuse, and mismanagement.

We found that GPO has made progress in addressing the considerations set forth in our 2022 report. GPO obtained approval to dispose of outdated Congressional publications at our distribution centers, creating space to bring in new customers. Aging computers at the Laurel Distribution Center (LDC) were replaced, Wi-Fi service was obtained for the Pueblo Distribution Center (PDC), and a mainframe inventory system migration plan was developed, facilitating the implementation of barcode scanning.

We conducted 14 OIG-101 presentations during this inspection, providing information designed to deter fraud, waste, and abuse to over 160 GPO employees.



Recommendations: Our report contained no findings or recommendations. We asked GPO to continue its focus on:

- Modernizing barcodes at the LDC and PDC.
- Improving hiring timelines, focusing on identified bottlenecks.
- Installing the emergency notification lighting system in the SPF production area.
- Installing hydrogen cyanide and carbon monoxide detectors on each production line located at SPF and Washington, DC.

Return on Investment: When fully implemented, GPO’s distribution center inventory processes will be more efficient and safer.



AUDITS

The Audits Division helps improve the management of GPO programs and activities by providing timely, balanced, credible, and independent audits that address GPO operations' economy, efficiency, and effectiveness. OIG audits are performed by Generally Accepted Government Auditing Standards issued by the Comptroller General of the United States.

Ongoing

Follow-up Audit on Telework and Transit Recommendations, Project No. A-2026-001

In January 2026, we initiated a follow-up audit of recommendations made in OIG Report No. 24-03, *Government Publishing Office Telework Program*. This is a self-initiated review to assess the effectiveness of management's actions in addressing prior audit issues.



Completed

Independent Auditors' Report on GPO Fiscal Year 2025 Consolidated Financial Statements, Report Number OIG-26-01, January 20, 2026

We contracted the independent public accounting firm of KPMG LLP (KPMG) to audit GPO's consolidated financial statements in accordance with U.S. generally accepted auditing standards. In the opinion of KPMG, the consolidated financial statements were fairly presented in all material respects, and the financial position of GPO as of September 30, 2025, was in accordance with U.S. generally accepted accounting principles.

Management Letter - Fiscal Year 2025 Consolidated Financial Statements Audit, Report Number OIG-26-02, January 20, 2026

In conjunction with the FY 2025 consolidated financial statements audit, KPMG considered GPO's internal controls over financial reporting. Accordingly, KPMG identified insufficient controls over personnel, commercial printing, and liability adjustment activities.



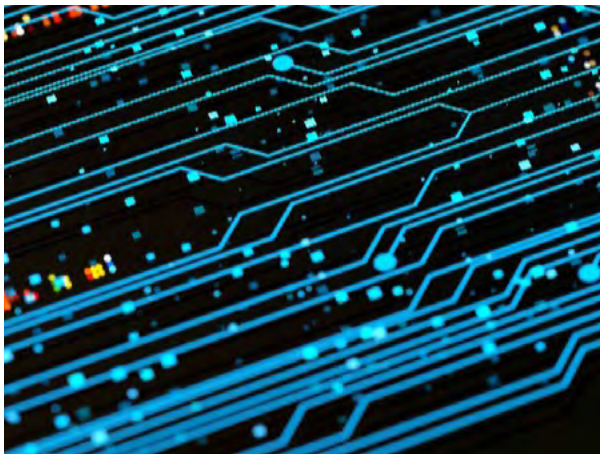
AUDITS (CONTINUED)

Completed (continued)

Cybersecurity Incident Response Maturity Assessment, Report Number OIG-26-06, March 30, 2026

In April 2025, we initiated a cross-cutting project with other Legislative Branch OIGs to evaluate the cybersecurity incident response capabilities of our respective agencies. Although GPO is not required to comply with the Federal Information Security Modernization Act (FISMA), GPO has adopted many of its practices and established cybersecurity policies and procedures aligned with industry standards. Our audit evaluated the maturity of GPO's incident detection, analysis, and handling processes using established FISMA Reporting Metrics.

Our audit found that GPO's policy lacked procedures for managing incident categories and standardized threat classifications based on characteristics, tactics, and potential impact. Analysis of more than 35,000 support system tickets further showed that GPO did not consistently adhere to its procedures for identifying, categorizing, and documenting computer security incidents. Additionally, the policy did not define detailed containment strategies or eradication procedures for various incident types. Based on FISMA Reporting Metrics, we concluded that GPO's incident detection and analysis capabilities align with the "Defined" maturity level, while its incident handling processes align with the "Ad Hoc" level.



Recommendations: We made three recommendations to address the lack of detailed policies and procedures, inconsistent documentation of computer security incidents, and inaccurate records within the service ticketing system.

Return on Investment: Enhancing GPO's policies will strengthen the organization's overall security posture by improving the speed and accuracy of incident detection and response. These updates will help ensure incidents are contained quickly, reducing operational risk and safeguarding mission-critical systems. Improving procedures for documenting incident response actions will also provide leadership with more reliable data, enabling clearer oversight, stronger performance measurement, and better-informed strategic decisions regarding cybersecurity investments.



INSPECTIONS

The Inspections Division reviews GPO programs and operations to identify opportunities to improve efficiency and effectiveness. These inspections are systematic and independent assessments of the design, implementation, and results of GPO's operations, programs, or policies. They provide timely, credible, and helpful information for agency managers, policymakers, and others. The GPO OIG's inspections are performed in accordance with the Quality Standards for Inspection and Evaluation issued by the Council of the Inspectors General on Integrity and Efficiency (CIGIE).

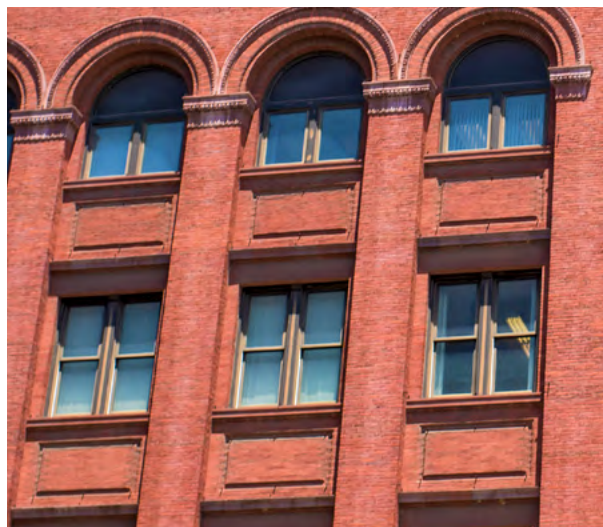
Ongoing

Human Capital Recruitment and Staffing Inspection, Project No. 26-02-CI

In December 2025, we initiated an inspection of Agency Human Capital's Recruitment and Staffing. This self-initiated inspection will determine if GPO hiring practices are aligned with applicable laws, rules, regulations, and standard operating procedures (SOPs), as well as determine what hiring metrics are captured and evaluated by Agency Human Capital and provide insight into any existing systemic problems.

Agency Force Protection and International Travel, Project No. 26-04-LS

In March 2026, we initiated an inspection of Agency Force Protection's (AFP) procedures and reports of foreign travel. This self-initiated review will assess AFP's guidance and procedures to account for and assist GPO security clearance holders in foreign locations during global events.



Completed

Review of Government Secure and Intelligent Documents Quality Control Procedures, Report No. 26-04, March 2, 2026.

At the Agency's request, we initiated an inspection in June 2025 of Government Secure and Intelligent Documents' (GSID) production of flawed US passports at the Stennis Secure Production Facility. The objective of the inspection was to assess GSID processes, procedures, and actions that led to the loss of substantial revenue through the production of faulty passports. We found quality controls were in place and generally effective. However, we found GSID should enforce and improve existing procedures to ensure the quality of Next Generation Passports. The full report was provided to GPO leadership and congressional committees of jurisdiction. However, the report contains sensitive information about GPO's GSID quality control procedures, preventing its public release.

Recommendations: We issued eight recommendations designed to improve GSID procedures. GPO concurred with all recommendations and has already taken corrective action to fully address five of those recommendations.

Return on Investment: When fully implemented, our recommendations will enhance management controls and improve program results.

INVESTIGATIONS

The Investigations Division investigates fraud, waste, and abuse in GPO programs and operations. Investigations may include possible wrongdoing by GPO contractors, employees, program participants, and others who commit crimes against GPO. Through prosecution, administrative action(s), and monetary recovery, investigations promote integrity, efficiency, and accountability.

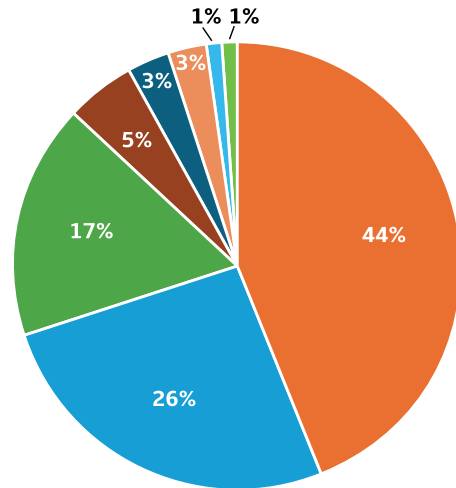
The Investigations Division (INV) conducts proactive and reactive criminal and administrative investigations. Investigations can derive from complaints or information from any person concerning violations of laws, rules, and regulations, mismanagement, gross waste of funds, abuse of authority, or a substantial and specific danger to public health and safety.

INV employs duly appointed criminal investigators with statutory authority to carry firearms, conduct arrests, execute search and seizure warrants, and perform other law enforcement duties. The INV team collaborates with internal and external OIG counterparts and other law enforcement partners.

OIG Intakes

The OIG receives allegations of wrongdoing by email, telephone, fax, mail, employee drop-box, and walk-ins. These are referred to collectively as "Intakes." INV reviews these allegations to determine whether the complaint should be the subject of an investigation, audit, inspection, or referred to GPO or another agency or organization. During this six-month reporting period, INV received 93 Intakes. There were 183 total Intakes in FY 2025.

Intake Breakdown



- Non-Substantive
- Other-Non-Criminal
- Fraud
- Time and Attendance
- Personnel Actions/Compensation
- Work Environment Complaints
- Employee Misconduct
- Management/EEO Issues

Investigative Statistics

Investigation Statistics	FY26	FY25
Intakes Received	93	183
Open Investigations (Active or Pending Closure)	6	11
Open Investigations (Pending Admin Action/Legal Outcome)	0	3
Investigations Initiated	3	11
Investigations Closed	10	8
Complaints Initiated	28	37
Management Referrals	4	13
Parties Referred for Suspension and/or Debarment	0	0
Referrals to Other Agencies	6	10

Status of Open Investigations (FY 26)

Status of Open Investigations	#
Open Investigations	6
Investigations Underway	6
Investigations Pending Prosecutorial Action	0
Investigations Pending Suspension and/or Debarment Actions	0
Investigations Pending Closure	0
Investigations Pending Other Administrative Action (corrective action)	0

CASE HIGHLIGHTS

Internal Investigation for Legislative Branch OIG (25-0012-I)

In August 2025, another Legislative Branch OIG asked for our assistance in investigating one of their employees for possible time-and-attendance fraud. The agency reported that the employee frequently left the office suite for long periods during business hours despite being scheduled to work. The investigation did not substantiate that the employee received pay for time they did not work. However, it determined that the employee violated the agency’s core work hours policy by departing the office earlier than permitted. Additionally, the investigation found that the employee occasionally used a mouse jiggler on their government-issued computer to prevent the screen from locking due to inactivity, in violation of multiple agency IT policies. As a result of the investigation, the employee received a five-day suspension from the requesting agency.

Return on Investment: This investigation reinforces accountability within the Legislative Branch OIG community. Though the investigation did not substantiate time-and-attendance fraud, it identified violations of core work hours and IT security policies, enabling the requesting agency to take corrective action against the employee. By providing timely investigative support and helping another OIG address misconduct, the investigation contributed to a more efficient stewardship of taxpayer resources.

Status: Closed February 10, 2026.

Report of Possible Bidder Collusion (24-0002-I)

Our office completed an investigation into allegations of bidder collusion involving bids submitted by the same individual on behalf of two companies. The investigation found that, although several bids from two companies originated from the same location, neither company was awarded the contract, and the Government incurred no financial loss. Additionally, investigators determined that, in certain circumstances, vendors may have agreements to share or use another vendor’s equipment, which does not prohibit them from competing for GPO contracts. Evidence showed that this arrangement applied in this case. As such, violations of 18 U.S.C. § 1343 – Fraud By Wire, Radio or Television, 18 U.S.C. § 371 – Conspiracy to Defraud the U.S., and 31 U.S.C § 3729-3733 – False Claims Act, were not substantiated. The U.S. Attorney’s Office declined prosecution for this matter.

Return on Investment: This investigation helped protect GPO’s procurement integrity by resolving serious allegations of bidder collusion. Although no violation of federal law or GPO Directive was identified, the effort served as a deterrent for future misconduct and provided investigators with valuable insights into the GPO’s procurement process.

Status: Closed March 9, 2026.

CASE HIGHLIGHTS (CONTINUED)

Proactive Investigation: GPO High-Valued Assets (25-0006-I)

We completed a proactive investigation into GPO's accounting of high-value assets, specifically laptop computers. The investigation aimed to uncover potential instances of theft of GPO equipment. A review of agency records revealed that GPO IT had conflicting asset-tracking information, resulting in inaccurate accounting records of GPO property. No evidence of theft was found. This matter was referred to OIG Audits and Inspections for consideration.

Return on Investment: This investigation identified weaknesses in GPO's asset-tracking processes. Though no evidence of theft was found, the discovery of conflicting records highlighted a significant internal control issue that could have led to future vulnerabilities. Ultimately, this effort safeguarded high-value government assets and underscored the need for improved accountability and property management within the agency.

Status: Closed March 9, 2026.



Proactive Investigation: Misuse of a GPO Government Vehicle (25-0007-I)

In July 2024, we initiated a proactive investigation into the use of GPO Government Vehicles. This investigation resulted from a larger proactive initiative that focused on analyzing vehicle history data. As a result, we identified a GPO vehicle with unexplained travel and isolated the vehicle's use to a single GPO employee. The investigation substantiated multiple incidents of vehicle misuse and concluded that the employee violated Title 31 U.S.C. § 1344 – Passenger Carrier Use. The subject of the investigation retired before the investigation was completed. The U.S. Attorney's Office declined prosecution for this matter.

Return on Investment: This investigation delivered a meaningful return on investment by demonstrating the effectiveness of proactive, data-driven oversight in identifying and addressing misuse of government resources. Although the subject retired prior to the investigation's conclusion, the effort still mitigated potential ongoing misuse, deterred similar conduct by others, and highlighted opportunities to strengthen internal controls and monitoring processes. Ultimately, the investigation protected taxpayer-funded assets, improved operational transparency, and reinforced stakeholder confidence in the integrity and use of government resources.

Status: Closed March 24, 2026.



CASE HIGHLIGHTS (CONTINUED)

Proactive Investigation: IT Cybersecurity Contract (25-0004-I)

We completed a proactive investigation into GPO's IT cybersecurity contract to assess whether the contractor was appropriately collecting, maintaining, archiving, processing, and solving cyber-related incidents. Investigators reviewed cybersecurity logs captured by the contractor and determined they were being retained properly. Further, the investigation disclosed that the contractor appropriately responded to cybersecurity alerts as required by the contract and processed them, including notifying GPO IT personnel when necessary.

Return on Investment: This proactive investigation reinforced the integrity of GPO's IT cybersecurity program. Although no contract violations or other misconduct were identified, the effort reinforced accountability for contractor performance, ensuring that GPO received the full value of its cybersecurity services, and strengthened stakeholder confidence in the agency's ability to safeguard sensitive systems.

Status: Closed March 30, 2026.

Proactive Initiatives

Our office continues to conduct several proactive investigative initiatives. Specifically, our ongoing efforts into the use of GPO government-owned vehicles have led to multiple substantiated investigations into vehicle misuse and highlighted internal control issues related to managing government vehicles within the GPO. Additionally, our proactive initiative to enhance GPO's inventory control of High-Value Assets, such as laptops, desktops, mobile devices, and other goods, has allowed our office to identify and deter risks of theft associated with their management. Our recently completed proactive investigation into GPO's cybersecurity contract promotes a culture of accountability and helps deter future misconduct. Planned proactive work includes collaboration with other OIG divisions and outreach with GPO management and staff.



OTHER INFORMATION

Whistleblower Retaliation Investigations.

None.

Instances of GPO Refusing to Provide Information or Assistance or Interfering with the OIG's Independence.

None.

Statutory Certification.

In accordance with the Legislative Branch Inspectors General Independence Act of 2019, as codified in 44 U.S.C. § 3903(c)(3), the Inspector General certifies that the GPO OIG has adequate safeguards and management procedures in place to ensure that the Investigations Division complies with the standards established by the Council of the Inspectors General on Integrity and Efficiency, which incorporate Department of Justice guidelines to ensure proper exercise of the statutory law enforcement authority.

Review of Legislation and Regulations.

During the reporting period, the GPO OIG continued its review of proposed legislation previously submitted to Congress by GPO and evaluated impact on the economy and efficiency of GPO programs and operations and the prevention and detection of fraud, waste, and abuse.



APPENDIX A. PEER REVIEW RESULTS

The following meets the requirement under 5 U.S.C. § 405 of the IG Act that Inspectors General include external peer review results in each Semiannual Report to Congress. Federal audit and inspection functions can receive a rating of “pass,” “pass with deficiencies,” or “fail.” Federal investigation functions can receive a rating of “compliant” or “noncompliant.”

Peer review reports are posted on our website at: <https://www.gpo.gov/who-we-are/our-agency/inspector-general/plans-and-reports>.

Peer Review of GPO-OIG Audit Function

The GPO OIG had no peer reviews of its audit function during this reporting period. The previous audit peer review was completed in March 2024, and the GPO OIG received a pass rating. This peer review report is posted on our website. The next audit peer review should occur in the 1st quarter of FY 2027.

Peer Review of GPO OIG Inspections Function

The GPO OIG had no peer reviews of its inspection function during this reporting period. The first inspection peer review is scheduled for the 3rd Quarter of FY 2026.

Peer Review of GPO OIG Investigative Function

The GPO OIG had no peer reviews of its investigative function during this reporting period. The previous investigative peer review was completed in April 2025, and the GPO OIG received a “compliant” rating. The peer review report is posted on our website. The next investigative peer review is scheduled to occur in the 4th quarter of FY 2029.

Peer Reviews conducted by GPO OIG

In March 2025, GPO OIG’s Inspections Division conducted a modified peer review of inspections and evaluations at the AmeriCorps OIG. This modified peer review required us to review only AmeriCorps OIG’s policies and procedures to determine compliance with the applicable Council of the Inspectors General on Integrity and Efficiency Quality Standards for Inspection and Evaluation (“Blue Book”) standards. The Inspections Division found AmeriCorps OIG’s policies and procedures were current and consistent with the December 2020 Blue Book standards.

APPENDIX B. NON-MONETARY RETURN ON INVESTMENT

Audits and Inspections	
Cybersecurity Incident Response Maturity Assessment (Report No. OIG-26-06)	
Benefit	Value
Improve processes and management controls	Enhancing GPO's policies will strengthen the organization's overall security posture by improving the speed and accuracy of incident detection and response. These updates will help ensure incidents are contained quickly, reducing operational risk and safeguarding mission-critical systems.
Improve compliance	Improving procedures for documenting incident response actions will provide GPO leadership with more reliable data, enabling clearer oversight, stronger performance measurement, and better-informed strategic decisions regarding cybersecurity investments.
Government Secure and Intelligent Documents Quality Control (Report No. 26-04)	
Benefit	Value
Improve program results	Implementing recommendations will strengthen internal quality controls and improve external support, reducing costs and errors.
Enhance management controls	Implementing recommendations will increase transparency, improve internal oversight, and share critical information within Government Secure & Intelligent Documents, thereby reducing errors.

Investigations	
Internal Investigation for Legislative Branch OIG (25-0012-I)	
Benefit	Value
Improve safety, morale, health, and security, and enhance stakeholder confidence	This investigation demonstrates that OIG employees are held to the highest standards and are accountable for their actions. By identifying and addressing misconduct, the investigation reinforced stakeholder confidence that the OIG's oversight mission applies to everyone in government—including those responsible for carrying it out.
Ensure Compliance and Oversight	This investigation strengthened oversight within the OIG community by uncovering violations of established policies for another Legislative Branch OIG. As a result, it promoted a culture of adherence to rules and ethical standards and sent a message that misconduct would be identified and addressed.

continued on page 16

Appendix B (continued)

Investigations (continued)	
Report of Possible Bidder Collusion (24-0002-I)	
Benefit	Value
Ensure Compliance and Oversight	Through this investigation, the OIG was able to thoroughly examine bidding activity and contractor relationships to confirm they aligned with federal law and GPO directives. The investigation promoted adherence to procurement requirements and enhanced confidence in the integrity of the oversight process.
Improve Safety, Morale, Health, and Security, and Enhance Stakeholder Confidence	By investigating allegations of collusion, the OIG demonstrated that it takes all procurement concerns seriously. Stakeholders gain confidence when even perceived irregularities are investigated thoroughly and professionally. Further, the investigation promotes a fair procurement process, boosting morale among vendors and GPO procurement staff.
Proactive Investigation: GPO High-Valued Assets (25-0006-I)	
Benefit	Value
Improve Systems and Processes	The investigation uncovered conflicting and inaccurate asset-tracking records within GPO. Through detection of these inaccurate records, the investigation delivered value by exposing a vulnerability that could lead to financial loss if left unaddressed.
Ensure Compliance and Oversight	The investigation ensures compliance and oversight by independently verifying the accuracy of GPO's asset records, identifying weaknesses in property-management controls, and promoting accountability for government equipment.
Misuse of a GPO Government Vehicle (25-0007-I)	
Benefit	Value
Improve Safety, Morale, Health, and Security, and Enhance Stakeholder Confidence	This investigation held employees accountable for the proper use of government resources. Identifying and addressing the misuse of a GPO vehicle mitigated potential safety and liability risks arising from unauthorized government vehicle operation.
Improve Systems and Processes	Through analysis of vehicle history data, the OIG identified weaknesses in accountability procedures that allowed misuse to go undetected over multiple years. As a result, GPO can implement more rigorous data analysis and enhance employee training on the proper use of government vehicles.
Ensure Compliance and Oversight	This investigation actively monitored adherence to federal regulations and agency policies governing the use of government vehicles. The OIG's detection of vehicle misuse demonstrates that oversight mechanisms are in place and effective.

Appendix B (continued)

Investigations (continued)	
Proactive Investigation: IT Cybersecurity Contract (25-0004-I)	
Benefit	Value
Validate Existing Processes	By validating that the contractor was properly collecting, retaining, and responding to cybersecurity incidents, the investigation provided assurance that GPO is receiving the protection it is paying for.
Ensure Compliance and Oversight	This investigation confirms that the contractor is meeting contractual requirements as expected. Additionally, proactively reviewing the contractor's performance ensured accountability and reduces the likelihood of fraud, waste, or poor performance.

APPENDIX C. INVESTIGATIONS STATISTICS

Investigation Statistics for Reporting Period⁷

Item	Quantity
Investigations Open at the Beginning of the Period	13
Investigations Opened during the Reporting Period	3
Investigations Closed during the Reporting Period	10
Investigations Open at the End of the Reporting Period	6
Complaints Open at the beginning of the Reporting Period	3
Complaints Opened during the Reporting Period	28
Complaints Closed during the Reporting Period	19
Complaints Open at the End of the Reporting Period	12
Referrals to Other Agencies	6
Referrals to Audits and Inspections Divisions	1
Proactive Initiatives Open at the Beginning of the Period	3
Proactive Initiatives Opened during the Reporting Period	0
Proactive Initiatives Closed during the Reporting Period	2
Proactive Initiatives Open at the End of the Reporting Period	1

Current Types of Open Investigations	Number	Percentage
Procurement/Contract Fraud	3	50%
Employee Misconduct	1	16.66%
Proactive Initiatives	1	16.66%
Time and Attendance Fraud	1	16.66%
Total	6	100%

⁷ Metrics were obtained from OIG's Case Management Tracking System.

Appendix C (continued)

Investigations Productivity Statistics for Reporting Period⁸

Item	No. or Amount
Arrests, including Summons in Lieu of Arrest	1
Persons Referred to DOJ for Criminal Prosecution	2
Persons Accepted for Criminal Prosecution	1
Persons Declined for Criminal Prosecution	1
Persons Referred to State/Local Prosecuting Authorities for Criminal Prosecution	0
Indictments/Information/Complaints	1
Initial Appearance	1
Convictions	0
Guilty Pleas/Deferred Prosecution Agreements	0
Criminal Fines, Fees, Recovery, and/or Restitution	0
Civil Settlements	0
Civil Fines, Fees, Recovery, and/or Restitution	\$676.30
Subpoenas Issued	0
Total Number of Investigative Reports Issued	3
Referrals to GPO Management for Possible Corrective Action and/or information Purposes	4
Parties Referred to GPO Management for Suspension and Debarment Action	0
Total Referrals to the Audits and Inspections Divisions	1
Discovered Material Loss to the Government	\$593.00

⁸ Metrics were obtained from OIG's Case Management Tracking System.

APPENDIX D. OPEN OIG RECOMMENDATIONS

Management Decisions This Reporting Period*

Date Issued	Name of Audit/ Inspection/Investigation	Report Number	Number of Open Recommendations	Monetary Impact
09/17/2024	Management of Excess and Obsolete Paper and Secure Documents	24-08	1	\$0
<p>Recommendation 24-08-02: 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.</p>				
10/31/2024	Physical Security Inspection	25-01	1	\$0
<p>Recommendation 25-01-07: Consider the purchase and installation of larger X-ray machines at loading docks.</p>				
03/21/2025	Fleet Management	25-07	1	\$0
<p>Recommendation 25-07-06: Develop and implement detailed standard operating procedures and checklists to verify that all disposition actions are completed within a defined period before marking a returned item as complete in the surplus property system.</p>				
06/05/2025	GPO Procured Printing Inspection	25-08	3	\$0
<p>Recommendation 25-08-01: Update the performance plans for the National Account Managers to include standards regarding proactive efforts to develop new customers, and ensure these standards are incorporated into the annual marketing plan.</p> <p>Recommendation 25-08-02: Develop a marketing plan to initiate contact with those agencies not currently doing business with GPO.</p> <p>Recommendation 25-08-03: Develop specific and measurable annual targets for customer and revenue growth.</p>				
06/16/2025	Management Implication Report: Government Cell Phone Applications	24-0014-I	3	\$0
<p>Recommendation 24-0014-I-01: Enroll all GPO-issued devices in a Mobile Device Management system capable of controlling application installations, limited to only approved applications, and enforcing policy compliance.</p> <p>Recommendation 24-0014-I-02: While the current annual GPO Cybersecurity Awareness Training highlights the risks of downloading mobile applications, we recommend that the annual training include more information about or greater emphasis on the prohibition of downloading personal or non-GPO software on GPO-issued mobile devices.</p> <p>Recommendation 24-0014-I-03: GPO should consider updating IT policies to more clearly define the scope of acceptable and prohibited uses, including establishing a “whitelist” of approved applications. The updated policy should better delineate reasonable personal use, use while off-duty, and the consequences for violations, including loss of network access or mobile phone use.</p>				

Appendix D (continued)

Date Issued	Name of Audit/ Inspection/Investigation	Report Number	Number of Open Recommendations	Monetary Impact
07/30/2025	Inventory Management	25-09	4	\$0
<p>Recommendation 25-09-01: Review GPO Instructions 810.5B, Organization and Functions of the Board of Survey, and 810.11B, GPO Property Management Program, for applicability and update or replace them with policies and standard operating procedures that align with the current organizational structure and business operations.</p> <p>Recommendation 25-09-02: Develop and implement comprehensive procedures for conducting inventory counts, regardless of physical storage location. These procedures should include, but not be limited to:</p> <ul style="list-style-type: none"> a. Establish accountability and responsibilities for the overall physical count. b. Standardize the frequency of counts and the method of selecting individual items or locations for the count. c. Document the count and supervisor review. d. Assess production paper and materials for obsolete, damaged, and slow-moving items for action. <p>Recommendation 25-09-03: Take appropriate action to pursue potential revenue opportunities for the 155 non-moving inventory items, valued at nearly \$304,000, in funds that can be put to better use, identified in this audit.</p> <p>Recommendation 25-09-04: Take appropriate action to remedy the \$39,000 overstatement in the inventory management system for the 44 inventory items identified in this audit.</p>				
08/21/2025	Federal Depository Library Program Assessments	25-10	4	\$0
<p>Recommendation 25-10-01: Resume conducting firsthand investigations, in accordance with Title 44 section 1909, paragraph 2.</p> <p>Recommendation 25-10-02: Update SOD 312 to include rubrics and definitions, along with a simple checklist, as a minimal firsthand investigation that executives can use during commemorative event trips.</p> <p>Recommendation 25-10-03: Request JCP approval for measures that are considered necessary for the economical and practical implementation of the FDLP, such as including commemorative events, training, or consultations as firsthand investigations.</p> <p>Recommendation 25-10-04: Develop and use a system of recordkeeping to track notifications to the JCP and JCP approval of SuDoc activities for the economical and practical implementation of the FDLP.</p>				
03/02/2026	Limited Scope Inquiry: Review of Government Secure & Intelligent Documents QC Procedures	26-04	3	\$0
<p>Recommendations 26-04-02, 26-04-03, and 26-04-07: Contact the GPO OIG Inspection Division for additional information.</p> <p>*Management Decision: GPO concurred with these recommendations.</p>				

Appendix D (continued)

Date Issued	Name of Audit/ Inspection/Investigation	Report Number	Number of Open Recommendations	Monetary Impact
03/30/2026	OIG Cybersecurity Incident Response Maturity Assessment	26-06	3	\$0
<p>Recommendations 26-06-01: Develop detailed procedures for the following areas:</p> <ul style="list-style-type: none"> a. Handling specific incident types during the Detection and Analysis phase b. Incident containment strategies for major incident types c. Incident eradication activities <p>Recommendation 26-06-02: Ensure that Triage Coordinators fully document key information in the incident ticket, including (1) the determination of whether or not the event is a computer security incident and (2) the steps taken for incident containment, eradication, and recovery.</p> <p>Recommendation 26-06-03: Ensure tickets identified in Tables 1 and 2 are correctly classified in the IT ServiceHUB.</p> <p>*Management Decision: GPO concurred with these recommendations.</p>				

APPENDIX E. STATUS OF OIG RECOMMENDATIONS

Number of OIG Recommendations Opened and Closed During this Reporting Period

Date Issued	Name	Report Number	Number of Recommendations Opened	Number of Recommendations Closed
09/28/2023	Top 10 Safety Hazards Program Inspection	23-08	0	1
02/14/2024	GPO Indoor Air Quality Inspection	24-02	0	3
10/31/2024	Physical Security Inspection	25-01	0	1
03/21/2025	Fleet Management	25-07	0	6
03/02/2026	Limited Scope Inquiry: Review of Government Secure & Intelligent Documents QC Procedures	26-04	8	5
03/30/2026	OIG Cybersecurity Incident Response Maturity Assessment	26-06	3	0
		Total	11	16

APPENDIX F. REPORTING REQUIREMENTS

Reporting Requirements under the IG Act of 1978

Reporting ⁹	Requirement	Page(s)
Section 4(a)(2)	Review of Legislation and Regulations	13
Section 5(a)(1)	Significant Problems, Abuses, and Deficiencies	5-12
Section 5(a)(1)	Recommendations for Corrective Actions to Address Problems, Abuses, and Deficiencies Identified	6-12
Section 5(a)(2)	Outstanding Recommendations on Which Corrective Action Has Not Been Completed	20-22
Section 5(a)(3)	Significant Investigations Closed	9-12
Section 5(a)(4)	Convictions Resulting from Investigations	19
Section 5(a)(5)	List of Completed Audit, Inspection, or Evaluation Reports	5-8, 14
Section 5(a)(6)	Management Decisions with Respect to Prior Audits, Inspections, or Evaluations	20-22
Section 5(a)(7)	Information described under section 804(b) of the Federal Financial Management Improvement Act of 1996 – Not applicable to GPO	N/A
Section 5(a)(8)-(10)	Peer Review Results	14
Section 5(a)(11)	Statistical Tables Related to Investigations	18-19
Section 5(a)(12)	Description of Metrics Used for Developing the Data for the Statistical Tables	18-19
Section 5(a)(13)	Substantiated Investigations Involving Senior Government Employees	N/A
Section 5(a)(14)	Description of Any Instance(s) of Whistleblower Retaliation	13
Section 5(a)(15)	Information Related to Any Attempt(s) by the Agency to Interfere with the Independence of the OIG	13
Section 5(a)(16)	Inspections, Evaluations, Audits, and Investigations Involving Senior Government Employees That Were Closed and Not Disclosed to the Public	8
44 U.S.C. § 3903(c)(3)	Certification of law enforcement standards	13

⁹ Public Law 117-263, James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, section 5273, Semiannual Reports. The National Defense Authorization Act (NDAA) amendments to section 5 modifying the reporting requirements in the IG Act are not yet codified in 5 U.S.C. § 405. Therefore, all references cite to the requirements as amended by the NDAA.

APPENDIX G. ABBREVIATIONS AND ACRONYMS

AFP	Agency Force Protection
CIGIE	Council of the Inspectors General on Integrity and Efficiency
DOJ	Department of Justice
FDLP	Federal Depository Library Program
FISM	Federal Information Security Modernization Act
FY	Fiscal Year
GPO	Government Publishing Office
GSID	Government Secure and Intelligent Documents
IG	Inspector General
IG Act	Inspector General Act of 1978, as amended.
INV	Investigations Division
IT	Information Technology
JCP	Joint Committee on Printing
KPMG	KPMG, LLC.
LDC	Laurel Distribution Center
NDAA	National Defense Authorization Act
OIG	Office of the Inspector General
PDC	Pueblo Distribution Center
ROI	Return on Investment
SOD	Superintendent of Documents (Policy)
SOP	Standard Operating Procedures
SPF	Stennis Secure Production Facility
SuDoc	Superintendent of Documents
Title 44	U.S.C. Title 44 – Public Printing and Documents, as amended
U.S.C.	United States Code

APPENDIX H. GLOSSARY OF TERMS

Abuse

The behavior that is deficient or improper when compared with behavior that a prudent person would consider reasonable and necessary business practice, given the facts and circumstances, but excludes fraud and noncompliance with provisions of laws, regulations, contracts, and grant agreements. Abuse also includes the misuse of authority or position for personal financial gain or for the financial interests of an immediate or close family member or business associate.

Complaint

The initial receipt of an allegation is documented immediately upon receipt; an allegation is then converted to a complaint within ten calendar days if the OIG can reasonably articulate a nexus to a violation of law, policy, practice, or a specific threat to human life, national security, or property. Complaints are then converted to full investigations within 30 days, provided there is reason to believe that a crime, tort, or policy violation within the OIG's jurisdiction has been developed; if not, the matter shall be closed.

Consideration

Suggest a corrective action to address potential deficiencies or problems. Considerations do not rise to the level of formal recommendations and are not tracked by the OIG.

Finding

The problem statement identified during an audit or inspection typically has criteria, conditions, causes, and effects.

Fraud

Fraud involves obtaining something of value through willful misrepresentation.

Indictment

The written formal charge of a crime by the grand jury is returned when 12 or more grand jurors vote in favor of it.

Intake

The OIG receives allegations of wrongdoing via email, telephone, mail, employee drop-box, and walk-ins.

Investigation

OIG conducts criminal, civil, and administrative investigations relating to violations of Federal laws, rules, or regulations pertaining to GPO programs, contracts, and operations. It also investigates allegations of criminal activity and serious misconduct by GPO employees. Fraud investigations typically result from allegations or suspicions of wrongdoing involving GPO programs, operations, or personnel. Investigations may also result from broad initiatives arising from previous OIG activities and interagency initiatives.

Management Decision

GPO management's evaluation of the findings and recommendations included in an audit report. Management issues a final decision concerning its response to such findings and recommendations, including actions concluded to be necessary.

Management Implication Report

A management report is issued during or after an investigation, identifying systemic problems or advising management of significant issues that require immediate attention.

Management Letter

A management letter describes the deficiencies in internal controls identified during the audit that do not rise to the level of seriousness to be stated in the final auditor's report.

Recommendation

Action is needed to correct or eliminate the recurrence of the cause of an identified finding.

Appendix H (continued)

Recommendation that Funds be Put to Better Use

A recommendation by the OIG that funds could be used more efficiently if GPO management took actions to implement and complete the recommendation, including—

- (A) reductions in outlays;
- (B) de-obligation of funds from programs or operations;
- (C) withdrawal of interest subsidy costs on loans or loan guarantees, insurance, or bonds;
- (D) costs not incurred by implementing recommended improvements related to the operations of the establishment, a contractor, or grantee;
- (E) avoidance of unnecessary expenditures noted in pre-award reviews of contract or grant agreements; or
- (F) any other savings that are specifically identified.

Return on Investment

Return on Investment (ROI) is a commonly used profitability ratio that measures the amount of return, or profit, an investment generates relative to cost. The ROI for an OIG is the most quantifiable performance metric and considers the cost of doing business and the revenues they collect.

Senior Government Employee

- (A) an officer or employee in the executive branch (including a special Government employee as defined in section 202 of title 18, United States Code) who occupies a position classified at or above GS-15 of the General Schedule or, in the case of positions not under the General Schedule, for which the rate of basic pay is equal to or greater than 120 percent of the minimum rate of basic pay payable for GS-15 of the General Schedule; and
- (B) any commissioned officer in the Armed Forces in pay grades O-6 and above.

Waste

Waste is using or expending resources carelessly, extravagantly, or for no purpose. Importantly, waste can include activities that do not include abuse and do not necessarily involve a violation of the law. Instead, waste relates primarily to mismanagement, inappropriate actions, and inadequate oversight.

REPORT FRAUD, WASTE, OR ABUSE

Report violations of law, rules, or agency regulations, mismanagement, gross waste of funds, abuse of authority, and danger to public health and safety related to GPO contracts, programs, and employees.

**U.S. Government Publishing Office
Office of the Inspector General
P.O. Box 1790
Washington, DC 20013-1790**

Email: gpoighotline@gpo.gov

Hotline: 866.4GPO.OIG (866.447.6644)









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

www.gpo.gov/oig/