Accessible Version

October 23, 2019

To: Gene L. Dodaro
Comptroller General of the United States

From: Adam R. Trzeciak
Inspector General

Subject: Semiannual Report to Congress—April 1, 2019, through September 30, 2019

I am pleased to submit this report in accordance with Section 5 of the Government Accountability Office Act of 2008. The report summarizes the activities of the Office of Inspector General (OIG) for the second reporting period of fiscal year 2019. The Act requires that you transmit the report to Congress within 30 days after receipt. Your transmittal should also include any comments you consider appropriate.

During this reporting period, we issued three audit reports. We also closed 6 investigations and opened 3 new investigations. In addition, we processed 73 hotline complaints, many of which were referred to other OIGs for action because the matters involved were within their jurisdictions. We remained active in the GAO and OIG communities by briefing new GAO employees on our audit and investigative missions, and participating in Council of Inspectors General on Integrity and Efficiency committees and working groups. Details of these activities and other OIG accomplishments are provided in the accompanying report.

We post our audit, evaluation, and semiannual reports on gao.gov and oversight.gov, a publicly accessible, text-searchable website containing the latest reports from contributing federal inspectors general. In addition, OIG reports are included in the listing of available updates on GAO's GovDelivery subscription page. We continue to look for innovative ways to enhance our oversight efforts and increase the transparency of our work.

I appreciate my team's dedication and professionalism in their continuing efforts to help GAO improve its operations. Their hard work and accomplishments are reflected in the attached report. I also thank GAO's Executive Committee, managers, and staff for their cooperation and attention to the important work of our office.

Attachments

INTRODUCTION

The United States Government Accountability Office

The U.S. Government Accountability Office (GAO) is an independent agency in the legislative branch of the federal government. GAO exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and ensure the accountability of the federal government for the benefit of the American people. It supports congressional oversight by (1) auditing agency operations to determine whether federal funds are being spent efficiently and effectively; (2) investigating allegations of illegal and improper activities; (3) reporting on how well government programs and policies are meeting objectives; (4) performing policy analyses and outlining options for congressional consideration; and (5) issuing legal decisions and opinions, such as bid protest rulings and reports on agency rules.

The Office of Inspector General

Established as a statutory office by the Government Accountability Office Act of 2008, GAO's Office of Inspector General (OIG) independently conducts audits, evaluations, and other reviews of GAO programs and operations and makes recommendations to promote economy, efficiency, and effectiveness in GAO. The OIG also investigates allegations of fraud, waste, and abuse, including the possible violation of law or regulation within GAO.

OIG STRATEGIC PUBLICATIONS

Strategic Plan

The OIG's Strategic Plan for Fiscal Years 2016-2020 identifies the vision, goals, objectives, and strategies for its activities under the authority of the Government Accountability Office Act of 2008, to promote efficiency, effectiveness, and integrity in GAO programs and operations. As discussed in the plan, the OIG supports GAO and Congress by helping to protect GAO programs and operations from fraud, waste, and abuse. Independent and objective audits, evaluations, and investigations are the primary methods for assessing GAO programs and operations and identifying risks to GAO, enhancing its ability to protect and maximize its resources.

Biennial Work Plan—Fiscal Years 2019 and 2020

The OIG's biennial work plan provides a brief description of audits and other work planned for fiscal years 2019 and 2020 and an overview of its investigations program. In addition, the plan sets forth OIG's formal strategy for identifying priority issues and managing its workload and resources.

Top Management Challenges Facing GAO

Each year, the OIG is asked to comment on management's assessment and reporting of GAO's challenges for its annual Performance and Accountability Report. OIG work has resulted in improved reporting and transparency of GAO's management challenges and the efforts under way to mitigate the risk these challenges pose to GAO's ability to efficiently and effectively support Congress and the American people. Progress in addressing these challenges is monitored through the agency's annual performance and accountability process and OIG audits and evaluations.

GAO continues to address mission challenges including (1) managing a quality workforce, (2) improving the efficiency of GAO engagements, and (3) ensuring the confidentiality, integrity, and availability of GAO's information technology services. The OIG identified infrastructure management as a potential challenge requiring appropriate attention. GAO's implementation of expanded telework has freed up space in its Headquarters building in Washington, D.C. The agency then initiated a space consolidation program with the intent to increase tenant occupancy. These efforts to maximize the use of GAO's building space and bring in revenue to offset rising costs have also resulted in expenditures related to development, approval, and implementation of the space consolidation plan.

Semiannual Reports to Congress

GAO OIG's Semiannual Reports to Congress describe the OIG's work on identifying problems, abuses, deficiencies, remedies, and investigative outcomes relating to the administration of GAO programs and operations that were disclosed during the reporting period. This semiannual report presents the results of the OIG's work for the reporting period April 1, 2019, through September 30, 2019, including product and performance statistics for audits and investigations. It also provides an overview of each audit report issued and actions GAO took or initiated in response to those audit reports, as of the end of the reporting period.

ACTIVITIES OF THE OFFICE OF INSPECTOR GENERAL

GAO and OIG management work cooperatively in fulfilling the role of the OIG. In that light, there were no attempts by GAO to resist, object to, or interfere with OIG independence or delay OIG access to information during the reporting period.

Timely resolution of outstanding recommendations continues to be a priority for both the agency and the OIG. GAO generally agreed with all recommendations, and provided agency comments within 60 days for OIG-19-1 issued in July 2019. However for two reports issued on or just before September 30, 2019, formal responses from management on concurrence are not due until the end of November 2019. Table 1 provides fiscal year summary statistics for unimplemented OIG recommendations as of September 30, 2019.

Table 1: Fiscal Year Summary Statistics Related to Unimplemented OIG Recommendations, as of September 30, 2019

Fiscal Year	Number of Reports with Unimplemented Recommendations	Number of Unimplemented Recommendations
2018	1	3
2019	2	9
Total	**3**	**12**

Source: OIG assessment as of September 30, 2019.

Audits and Evaluations

All OIG audit and evaluation reports, with the exception of reports on GAO's compliance with requirements of the Federal Information Security Modernization Act of 2014 (FISMA), are fully disclosed to the public. Due to the sensitive nature of issues identified, generally only summary pages of the FISMA report are made publicly available.

OIG Reports and Status of Current Period Recommendations, and Other Work

The OIG issued three audit reports (OIG-19-1, OIG-19-2, and OIG-19-3) containing a total of 15 recommendations during the period. GAO generally agreed with the recommendations in each report; however, as mentioned previously, formal responses from management on concurrence with recommendations are not due until the end of November 2019 on the two most recent reports. During the audit of Telework Participation and Eligibility (OIG 19-1), the OIG worked with management to close three recommendations prior to report issuance. Subsequent to completion of fieldwork on the audit of the DATA Act submission for the first quarter of fiscal year 2019, GAO took actions to address the intent of the three recommendations (OIG-19-2). The OIG verified successful implementation for two of the recommendations. To address the third recommendation, GAO assigned new program activity codes to ensure obligations are allocated to the proper project and fund group. GAO expects to implement these new program activity codes for DATA Act reporting purposes by November 2019.

Table 2 identifies each report issued during the period, its objective, and the number and status of recommendations made, as of September 30, 2019. See attachment II for a summary of each audit report issued during the current reporting period. OIG reports are available at gao.gov and oversight.gov.

Table 2: Status of Agency Actions on OIG Audit Reports Issued in Current Reporting Period (April 1, 2019, through September 30, 2019)

OIG Reports	Audit Objective	Number of Recommendations	Status of Recommendations
TELEWORK PARTICIPATION AND ELIGIBILITY: Additional Controls Are Needed to Strengthen Compliance with Telework Act Requirements and GAO Policies for Certain Employees, OIG-19-1 (July 15, 2019)	To evaluate the extent to which GAO established effective controls to comply with the Telework Act and GAO's policies regarding telework eligibility and participation requirements for certain employees.	Four	**Closed/Implemented** GAO has taken actions to address the intent of the recommendations. During the course of the engagement, the OIG worked with management to close three recommendations involving establishing clearer guidance for managers to use in deciding whether to cancel telework arrangements and internal controls to prevent interns from teleworking. In August 2019, GAO addressed the fourth recommendation by establishing and documenting eligibility criteria for re-employed annuitants, consultants, and senior managers.
DATA Act: Audit of GAO's Fiscal Year 2019, First Quarter, DATA Act Submission, OIG-19-2 (September 27, 2019)	To assess (1) the completeness, timeliness, quality, and accuracy of fiscal year 2019 first quarter financial and award data submitted by GAO for publication on USASpending.gov and (2) GAO's implementation and use of the government-wide financial data standards established by OMB and Treasury.	Three	**Two Closed, One In-Progress** GAO took action to address the intent of the three recommendations. The OIG verified successful implementation for two of the recommendations. GAO expects to fully implement the third recommendation by November 2019. The OIG expects to receive management's final response regarding its corrective actions for the open recommendation within 60 days of report issuance.

OIG Reports	Audit Objective	Number of Recommendations	Status of Recommendations
INFORMATION SECURITY: Review of GAO's Program and Practices for Fiscal Year 2018, OIG-19-3 *(September 30, 2019)*	To evaluate the extent to which GAO has complied with Federal Information Security Modernization Act of 2014 (FISMA) requirements.	Eight	**Open/In-Progress** In its written comments to the report, GAO stated that it had initiated actions to address the majority of the recommendations. The OIG expects to receive management's final response regarding its corrective actions within 60 days of report issuance.

Source: OIG assessment as of September 30, 2019.

Status of Prior Period Unimplemented OIG Audit Recommendations

At the end of the prior reporting period (March 31, 2019), there were three unimplemented recommendations from the audit of GAO's information security program for fiscal years 2016 and 2017. During the current period the recommendations remained open. Table 3 summarizes the status of actions planned or taken in response to recommendations made in prior reporting periods, as of September 30, 2019.

Table 3: Status of Agency Actions on Prior Period Unimplemented OIG Recommendations, as of September 30, 2019

OIG reports	Recommendations	Status of actions planned or taken by GAO in response to the recommendations
INFORMATION SECURITY: Review of GAO's Program and Practices for Fiscal Years 2016 and 2017, OIG-18-4 (July 17, 2018)	Document and implement a process to evaluate current and future enterprise Information Technology (IT) investment portfolio assets, including risks, and ensure alignment with GAO's IT strategy for fiscal years 2017-2019.	**Recommendation: Open** GAO is working to finalize its Enterprise Risk Management Program Plan and develop implementation procedures to ensure IT investments support GAO's Strategic Plan and IT strategy, monitor progress towards achieving IT strategic objectives, and effectively manage IT risk at the enterprise level. GAO expects to complete this work by January 31, 2020.
	Document plans, policies, and procedures for identifying, prioritizing, and mitigating operational risk related to establishing full failover capabilities at the Alternate Computing Facility (ACF) in the event of a disaster and preparing for end-of-support upgrades for Windows 7.	**Recommendation: Open** GAO continues to work on contingency efforts, which includes replacement of the agency's current virtual desktop infrastructure (VDI) and migration from the Windows 7 operating system to the Windows10 operating system. This work is part of GAO's planned efforts to move VDI from the primary computing facility to the alternate computing facility, which has more robust contingency capabilities. Extended support for Windows 7 ends on January 14, 2020.
	Document and implement a process to identify and track hardware and software interdependencies for GAO's system inventory, including vendor support data such as end-of-life or end-of-support dates.	**Recommendation: Open** GAO has developed a software inventory and established a process for tracking end-of-life or end-of-support dates. Final implementation in terms of fully updating the inventory and respective data fields is in process and is expected to be completed in the first quarter of fiscal year 2020.

Source: OIG assessment as of September 30, 2019.

Complaints and Investigations

The OIG hotline is the primary source of complaints or information for identifying suspected fraud and other problems, abuses, and deficiencies relating to the administration of GAO's programs and operations. As shown in Table 4, the OIG processed 73 hotline complaints during this 6-month reporting period.

Table 4: Summary of OIG Hotline Complaint Activity, April 1, 2019 through September 30, 2019

Hotline complaints open at the start of the reporting period	0
New hotline complaints received this reporting period	73
Total hotline complaints	**73**
Complaints closed (referred to other GAO offices)	21
Complaints closed (referred to FraudNet[a])	0
Complaints closed (no jurisdiction and referred by the GAO/OIG to appropriate agency OIG or other law enforcement offices[b])	41
Complaints converted to investigations	3
Total hotline complaints open at the end of the reporting period	**8**

Source: OIG hotline summary statistics as of September 30, 2019.

[a]FraudNet is a government-wide hotline operated by GAO staff on its Forensic Audits and Investigative Service team that receives complaints of fraud, waste, abuse, and mismanagement of federal funds.

[b]FraudNet was provided a copy of each referral made outside of GAO.

In addition to the 73 hotline complaints shown in Table 4, the OIG received 59 complaints that were closed due to insufficient information or no basis for opening an investigation. These complaints generally did not involve GAO programs and operations, and lacked either (1) sufficient merit to warrant direct OIG referral to another federal or state organization, or (2) actionable information.

As shown in Table 5, there were 15 open investigations during this reporting period. At the end of the reporting period, nine investigations remained open. During the reporting period, the OIG issued four administrative subpoenas for records maintained by organizations external to GAO and one Report of Investigation, and referred three investigations for criminal prosecution.

Table 5: Summary of OIG Investigations, April 1, 2019 through September 30, 2019

Investigations open at the start of the reporting period	12
New investigations initiated this reporting period	3
Total Investigations	**15**
Investigations closed this reporting period	6
Total investigations open at the end of the reporting period	**9**
Total investigative reports issued during reporting period	**1**
Referred to Department of Justice	3
Referred to state/local prosecutor	0
Total referrals for criminal prosecution	**3**
Total indictments/information obtained during reporting period	**0**

Source: OIG investigative activity statistics as of September 30, 2019.

Investigations Not Disclosed Publicly

The six investigations closed during the period were not previously disclosed publicly. In addition, one report of investigation was issued (#7), and management provided preliminary information on its disposition. The OIG will close this investigation when management provides GAO with a final action report. A summary of these investigations is provided in Table 6 below.

Table 6: Closed/Pending Investigations Not Previously Disclosed Publicly, April 1, 2019, to September 30, 2019

Subject	Results	Completed
1. Telework and Time & Attendance Fraud The OIG received a hotline complaint alleging that an SES director committed time and attendance fraud, telework fraud, and a violation of Generally Accepted Government Auditing Standards (GAGAS). (G-18-0019-HL-O) (GS-15 or above equivalent)	The investigation was unable to validate that the GAO director committed time card fraud, telework fraud, GAGAS violations, or abuse of power. However, the investigation identified 95 days (66 partial days and 29 full days) in which the director claimed telework but did not log on to the GAO network. The OIG's Report of Investigation was forwarded to GAO's Human Capital Office. It indicated that no disciplinary action would be taken as the director's telework agreement had already been revoked. The subject subsequently retired in June 2019.	**April 26, 2019**
2. Telework and Time & Attendance Fraud The OIG was contacted by a GAO supervisor alleging that an analyst was committing time and attendance fraud by engaging in outside activities while working for GAO. (G-17-0220-HL-O)	The OIG's review of the analyst's time and attendance records showed that the employee violated GAO's Telework Order, which required the subject to spend 14 hours per pay period at the Official Duty Station. The OIG was unable to conclude whether the subject engaged in outside activities because the analyst resigned from GAO during investigative fieldwork. As a result, the investigation was closed.	**May 17, 2019**
3. Fictitious Documents The OIG received an email that a Senior Analyst verified employment and provided false tax records and pay stubs for a friend who was not a GAO employee to help the friend obtain a mortgage. (G-17-0221-O)	The investigation found that the Senior Analyst falsely represented to a mortgage lender that a loan applicant was an employee of the analyst's accounting business in an attempt to secure a $332,500 mortgage. The analyst pled guilty to one count of False Statement in Loan and Credit Application, in violation of Title 18, United States Code, Section 1014. On June 4, 2019, the analyst was sentenced to 2 years of supervised release and 100 hours of community service and was required to pay a fine of $1,000 and a special assessment of $100. Information about the conviction was referred to the analyst's state licensing organization.	**June 17, 2019**

Subject	Results	Completed
4. Unauthorized Database Access The OIG received an email from Lexis-Nexis expressing concern that an Administrative Assistant may have misused GAO's Lexis-Nexis account by conducting six unauthorized searches. (G-19-0019-O)	The investigation substantiated allegations that the Administrative Assistant's searches were for non-permissible reasons. Further, the investigation revealed that the subject had been making non-permissible searches for at least 10 years and conducted over 4,000 searches for personal reasons. The OIG issued a Report of Investigation to GAO's Human Capital Office on March 25, 2019. On May 28, 2019, GAO proposed a 3-day suspension which was later reduced to a 2-day suspension.	**June 18, 2019**
5. Threats The OIG received emails from GAO and contractors alleging that a facilities management specialist threatened contractor employees. (G-19-0184-P)	This matter was referred to GAO's Human Capital Office as a performance issue within management's purview.	**June 21, 2019**
6. Time and Attendance Fraud The OIG received a hotline complaint that a contract specialist falsified her timesheets, was insubordinate, and was abusing substances. (G-19-0160-HL-P)	The subject of the investigation separated from GAO during investigative fieldwork. The investigation was then closed.	**September 17, 2019**
7. Fraudulent Receipt of Benefits and Failure to Report The OIG received a hotline complaint that an Information Technology (IT) analyst had fraudulently received Social Security disability benefits while working for GAO; filed for bankruptcy twice without reporting it to GAO; and omitted debts on the analyst's financial disclosure report. (G-18-0069-HL-O)	The investigation determined that, while employed by GAO, the analyst fraudulently received Social Security benefits in 2009, 2010, and 2011. The analyst admitted to being overpaid $35,000 in Social Security benefits; failing to notify GAO of bankruptcies in 2012 and 2017; and inaccurately reporting debts on financial disclosure forms for 7 of the 9 years that GAO has employed the analyst. The Human Capital Office notified the OIG that GAO is planning to take disciplinary action in the coming weeks. OIG will provide a follow-up in the next semi-annual report.	**Pending final action.**

Source: OIG investigative activity statistics as of September 30, 2019.

Matters Referred for Prosecution

During the period, the OIG led a task force involving a phishing attempt to divert several high-level GAO officials' paychecks as well as the paychecks for high-level officials from other federal and state agencies. The task force includes the OIGs for the Federal Housing Finance Agency, Department of Energy, National Archives and Records Administration, and National Endowment

for the Humanities. Other task force members include the Secret Service, FBI, and Maryland State Police. The matter was accepted for prosecution by the U.S. Attorney's Office. The investigation is ongoing. (G-19-0077-O)

The OIG is investigating a senior manager (G-18-0248-O) and a senior staff (G-18-0191-HL-O) for alleged conflict of interest violations. The OIG is awaiting acceptance or declination decisions as of September 30, 2019.

Matters for Management Consideration

On March 29, 2019, the OIG issued an alert to GAO management based on vulnerabilities identified during its investigation (#4 in Table 6 above) into a privacy incident due to unauthorized database access by a GAO employee. The management alert contained three matters for management consideration to address the vulnerabilities and to help GAO more fully implement federal and GAO information security requirements in systems and services provided to GAO by external service providers. In its response dated May 28, 2019, GAO stated (1) it did not believe that the circumstances required GAO to notify individuals potentially affected by the security incident; (2) it had cancelled its general subscription to LexisNexis in December of 2018 and closely vets users of all subscription databases that contain personally identifiable information (PII); and (3) it has instituted a new form for employees requesting use of subscription databases containing PII and will review Privacy Impact Assessments every 3 years.

Other Activities

Activities within GAO

In July 2019, the Inspector General (IG) and Assistant IG for Audit met with the Auditor General and senior staff from the People's Republic of China for a discussion of audit practices and challenges, and the role of GAO's IG. OIG Counsel briefed participants attending GAO's International Auditor Fellowship Program (IAFP) on the history, role, and work of GAO's Office of Inspector General. The IAFP hosts middle-to-senior level professionals from supreme audit institutions worldwide in an effort to help these institutions to fulfill their missions and to enhance accountability and governance.

OIG leadership continued its discussion of the duties, responsibilities, and authorities of the OIG with participants in GAO's new employee orientation program. The IG and a senior investigator provided briefings to GAO mission teams on the OIG's investigations program, including investigative outcomes.

In addition, OIG leadership attends weekly senior staff meetings, and meets periodically with staff of the independent public accounting firm conducting GAO's annual financial statement audit and the Audit Advisory Committee.

Activities within the Inspector General Community

The OIG continued to participate on the Council of Inspectors General on Integrity and Efficiency (CIGIE), a council of federal inspectors general that promotes collaboration on issues of economy, efficiency, and effectiveness that transcend individual agencies. OIG leadership regularly participated in monthly CIGIE meetings, quarterly Legislative Branch Inspectors General meetings, and periodic meetings with other OIGs designed to address issues common to smaller OIGs. The Assistant Inspector General for Investigations (AIGI) participated in monthly CIGIE Investigations Committee meetings, quarterly AIGI meetings, and various investigative working groups. The Counsel to the Inspector General participated

in monthly CIGIE Legislation Committee meetings and Council of Counsels to Inspectors General meetings.

In addition, the OIG responded to requests from OIGs for support in developing internal operating policies and procedures. The OIG continues to increase public access to and transparency of its work by posting audit, evaluation, and semiannual reports on gao.gov and oversight.gov. Oversight.gov is a publicly accessible, text-searchable website containing public reports from contributing federal Inspectors General who are CIGIE members.

Freedom of Information

During the current reporting period the OIG received and processed one access request under GAO's access regulation, 4 C.F.R. Part 81.

Whistleblower Retaliation

The GAO IG has no statutory authority to investigate allegations of whistleblower retaliation. Although GAO is not subject to the Whistleblower Protection Act or the Whistleblower Protection Enhancement Act, GAO personnel management system controls are intended to protect GAO employees from prohibited personnel practices.

Telework Participation and Eligibility

In 2017, 91 percent of GAO's employees participated in the telework program. GAO's telework program supports several agency objectives, including emergency readiness and continuity planning, and work/life balance for employees. The objective of the audit was to evaluate the extent to which GAO established effective controls to comply with the Telework Enhancement Act of 2010 (the Telework Act) and GAO's policies regarding telework eligibility and participation requirements for certain employees. The Telework Act instructs agencies to establish a policy under which eligible employees of the agency are authorized to telework; determine the eligibility for all employees of the agency to participate in telework; and notify all employees of their eligibility to telework. Agencies must meet these requirements when implementing their telework programs.

GAO telework policies provide for the use of management discretion in allowing telework for employees with unacceptable performance and misconduct rising to the level of disciplinary and adverse actions. However, GAO lacked practical guidance to assist managers in their consideration of the appropriateness of continued telework participation in such cases—which could limit transparency, consistency, and fairness in decisions throughout the agency. The OIG also found some areas where internal controls were insufficient to prevent ineligible employees from obtaining telework arrangements or teleworking.

The OIG made four recommendations, which GAO has implemented. The recommendations focused on the need to establish clearer guidance for managers to use in deciding whether to cancel telework arrangements and internal controls to prevent ineligible employees from teleworking. The OIG also recommended that GAO establish eligibility criteria for re-employed annuitants, consultants, and senior managers participating in the telework program.

Digital Accountability and Transparency Act of 2014 (DATA Act)

The DATA Act requires federal agencies to report their spending data via USASpending.gov to make it more transparent to the public. The OIG contracted with the independent public accounting firm of Williams Adley to assess (1) the completeness, timeliness, quality, and accuracy of GAO's fiscal year 2019 first quarter financial and award data submitted for publication on USASpending.gov and (2) GAO's implementation and use of the government-wide financial data standards established by the Office of Management and Budget (OMB) and the Department of the Treasury (Treasury), as required by the DATA Act of 2014. The audit found that GAO's submission was timely, complete, and of high quality, adhering to the data standards established by OMB and Treasury. The report contains three recommendations intended to ensure the continued accuracy and compliance of GAO's DATA Act submissions, including procedures to ensure that spending data is properly categorized and accurately reflected on USASpending.gov. GAO agreed with the report findings and recommendations, and indicated that it has implemented the necessary corrective actions.

Information Security

The Federal Information Security Modernization Act of 2014 (FISMA) requires federal agencies to develop, document, and implement an agency-wide information security program for the information and systems that support their operations and assets, including those provided or managed by another agency or contractor. Although GAO, as a legislative branch agency, is not subject to FISMA, it has chosen to use FISMA as a set

of best practices for its information security program. GAO has implemented an information security program that is generally aligned with FISMA, but the OIG identified opportunities for GAO to improve the implementation of its information security program and to ensure consistency with federal best practices.

The OIG found the design of GAO's enterprise risk management program is largely consistent with National Institute of Standards and Technology (NIST) guidance although GAO has not fully implemented controls in the areas of Risk Management Strategy, Risk Assessment, and Supply Chain Risk Management. Additionally, GAO has generally established information protection policies that are consistent with federal best practices but has not consistently implemented these policies and procedures. For example, GAO regularly scans its environments to discover vulnerabilities such as misconfigurations and missing patches. However, critical and high-priority vulnerabilities were not always remediated in a timely fashion. Also, GAO policies call for establishing baseline configurations that can be used to configure machines securely and detect changes in the environment, but many were not documented.

The OIG also identified opportunities for GAO to improve disaster recovery planning. GAO did not conduct a disaster recovery plan test in fiscal year 2018, and one high-impact system did not have a contingency plan defined. Finally, GAO did not complete a business impact analysis, which helps to inform contingency planning decisions.

The OIG made eight recommendations to strengthen GAO's information security program and practices that encompassed risk management, security impact assessments, remediation of scan-identified vulnerabilities, baseline configuration documentation and approval, contingency planning, and business impact analysis.

OIG Mission

Our mission is to protect GAO's integrity through audits, investigations, and other work focused on promoting the economy, efficiency, and effectiveness in GAO programs and operations, and to keep the Comptroller General and Congress informed of fraud and other serious problems relating to the administration of GAO programs and operations.

Reporting Fraud, Waste, and Abuse in GAO's Internal Operations

To report fraud and other serious problems, abuses, and deficiencies relating to GAO programs and operations, you can do one of the following (anonymously, if you choose):

- Call toll-free (866) 680-7963 to speak with a hotline specialist, available 24 hours a day, 7 days a week.
- Visit https://OIG.alertline.com.

Obtaining Copies of OIG Reports and Testimonies

To obtain copies of OIG reports and testimonies, go to GAO's website: https://www.gao.gov/ig/ or https://www.oversight.gov/reports, created by the Council of Inspectors General on Integrity and Efficiency.