Office of the Inspector General
U.S. Government Accountability Office

INFORMATION SECURITY

Evaluation of GAO's Program and Practices for Fiscal Year 2012

Serving the Congress and the Nation

OIG-13-2

Office of the Inspector General
U.S. Government Accountability Office
Report Highlights

February 2013

INFORMATION SECURITY

Evaluation of GAO's Program and Practices for Fiscal Year 2012

What We Found

The Federal Information Security Management Act of 2002 (FISMA) requires that each federal agency establish an agency-wide information security management program for the information and information systems that support the agency's operations and assets. GAO is not obligated by law to comply with FISMA or Executive Branch information policies, but has adopted them to help ensure physical and information system security. Our prior year evaluations have shown that GAO has established an overall information security program that is generally consistent with the requirements of FISMA, OMB implementing guidance, and standards and guidance issued by the National Institute of Standards and Technology. For example, GAO has well defined operational and technical controls for remote access to its network. Its telecommunications policy requires users to sign rules of behavior and user agreements that acknowledge their responsibility and accountability. GAO also has a process for reporting and disabling lost or stolen devices to prevent unauthorized access. In addition, GAO has continued its focus on closing prior year security-related recommendations.

Our fiscal year 2012 limited evaluation reinforced our prior conclusion. However, using 18 new FISMA reporting metrics for federal inspectors general, we identified areas for improvement in the contingency planning process. We also identified resource challenges that affect GAO's ability to implement security upgrades and strategies identified by GAO managers and the OIG.

What We Recommend

To help strengthen GAO's overall information security program, we recommend that the Chief Information Officer take the following two actions: (1) implement measures to increase the redundancy and availability of GAO mission-essential applications and (2) develop and provide, for GAO senior management consideration, a proposed strategy to ensure power redundancy to GAO servers and provide a long-term alternate power supply in the event of a power outage. GAO concurred with our recommendations.

OIG
Office of the Inspector General

United States Government Accountability Office

Memorandum

Date: February 13, 2013

To: Comptroller General Gene L. Dodaro

From: Inspector General Adam Trzeciak

Subject: Information Security: Evaluation of GAO's Program and Practices for Fiscal Year 2012

We have completed a limited-scope, independent evaluation of the effectiveness of GAO's information security program and practices for fiscal year 2012 as prescribed by the Federal Information Security Management Act of 2002 (FISMA).[1] FISMA requires federal agencies to develop, document, and implement an agency-wide information security program to provide security for the information and information systems that support their operations and assets, including those provided or managed by another agency, contractor, or other source. In addition, each agency is required to have an annual independent evaluation of its information security program and practices, including control testing and compliance assessment, which is to be performed by the agency Inspector General (IG) or by an independent external auditor. GAO is not obligated by law to comply with FISMA or executive branch information policies, but has adopted them to help ensure physical and information system security.

Our prior year evaluations have shown that GAO has established an overall information security program that is generally consistent with the requirements of FISMA, OMB implementing guidance, and standards and guidance issued by the National Institute of Standards and Technology (NIST).[2] Our fiscal year 2012 limited review reinforced our prior conclusion, although this year, we identified areas for improvement in the contingency planning process. We also identified resource challenges that impact GAO's ability to implement security upgrades and strategies identified by GAO managers and the OIG. This report includes recommendations to help the agency more fully implement federal information security requirements for these program elements.

[1] Enacted as Title III of the E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002).

[2] GAO/OIG, *Information Security: Evaluation of GAO's Program and Practices for Fiscal Year 2010*, GAO/OIG-11-3 (Washington, D.C.: Mar. 4, 2011).; and *Information Security: Evaluation of GAO's Program and Practices for Fiscal Year 2011*, GAO/OIG-12-2 (Washington, D.C.: Mar. 30, 2012).

Objectives, Scope, and Methodology

For fiscal year 2012, we performed a limited FISMA evaluation of GAO's information security program and practices. Specifically, we assessed GAO's compliance with the 18 new FISMA metrics for fiscal year 2012 developed by the Department of Homeland Security (DHS) for reporting by executive agency Inspectors General,[3] rather than the complete list of DHS metrics as in prior years. These metrics established minimum and target levels of performance for administration priorities and metrics for other key performance areas that were designed to focus federal agency efforts on network security. Our review included the following eight information security areas: Configuration Management, Identity and Access Management, Incident Response and Reporting, Risk Management, Security Training, Plan of Action and Milestones (POA&M), Remote Access Management, and Contingency Planning. (See attachment I.)

We also evaluated changes to GAO systems, policies, and procedures in fiscal year 2012 that could potentially affect GAO's information security program. To assess GAO's performance for these areas, we analyzed the agency's information security policies, procedures, and guidance; interviewed staff in GAO's Information Systems and Technology Services (ISTS) office; and obtained additional data and documentation from them. In addition, we reviewed the security control documentation for GAO systems using a risk-based approach. As part of our review of Contingency Planning, we toured the Local Area Network Operations Center (LOC), visually inspected electrical circuits, and physically traced power cords for servers to check for power redundancy. Finally, we identified actions taken in response to past FISMA recommendations and determined if any of these recommendations can be closed.

We conducted this evaluation from December 2012 to February 2013 in accordance with the *Quality Standards for Inspection and Evaluation* established by the Council of the Inspectors General on Integrity and Efficiency, in January 2012. Those standards require that we plan and perform the evaluation to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our evaluation objectives.

Background

To help protect against threats to federal systems, FISMA sets forth a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets. Its framework creates a cycle of risk management activities necessary for an effective security program. It is also intended to provide a mechanism for improved oversight

[3] U.S. Department of Homeland Security, *FY 2012 Inspector General Federal Information Security Management Act Reporting Metrics*, (March 6, 2012).

of federal agency information security programs. In order to ensure the implementation of this framework, FISMA assigns specific responsibilities to OMB, agency heads, chief information officers (CIO), inspectors general, and NIST. OMB is tasked with developing and overseeing the implementation of policies, principles, standards, and guidelines on information security; reporting at least annually on agency compliance with the act; and approving or disapproving agency information security programs. Agency heads are tasked with providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of the agency. Agency heads and CIO are tasked with developing, documenting, and implementing agency-wide information security programs. Inspectors general are tasked with conducting annual independent evaluations of agency efforts to effectively implement information security. NIST is tasked with providing standards and guidance to agencies on information security.

Changes to GAO Control Environment during Fiscal Year 2012

ISTS did not retire any existing FISMA systems or add any new FISMA systems in fiscal year 2012. Therefore, the GAO FISMA inventory remained unchanged from fiscal year 2011. During fiscal year 2012, ISTS implemented software upgrades including Microsoft Office 2007 and Oracle 11G. We reviewed configuration management documentation and verified that these changes were authorized and approved.

Improvements Needed to Fully Implement Security Program

GAO has established an information security program that is generally consistent with federal requirements, guidance, and standards. Of particular note in fiscal year 2012, ISTS updated procedures for managing and tracking annual security awareness training and role-based training to more accurately report compliance and ensure accountability for the required training. The recently developed Mandatory Training Portal allows ISTS managers to track who has completed information security awareness and role-based training. It also allows portal administrators to send automated e-mail notifications to those who have not yet satisfied the requirement. GAO reported that awareness training compliance was at 99 percent and the role-based training compliance was at 98 percent.

GAO also has well-defined operational[4] and technical[5] controls for Remote Access Management. For example, GAO has a published telecommuting policy that requires

[4] Operational controls are safeguards or countermeasures for an information system that are primarily implemented and executed by people (as opposed to systems).

[5] Technical controls are safeguards or countermeasures for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.

users to sign rules of behavior and user agreements that acknowledge their responsibility and accountability. GAO also has a process for reporting and disabling lost or stolen devices to prevent unauthorized access. We reviewed documentation from an actual lost property incident and verified that ISTS personnel followed these procedures.

However, information security threats change almost daily, requiring constant diligence and oversight to mitigate possible impact on information availability, integrity, and continuity. In evaluating elements of this program based on the DHS reporting metrics for Inspectors General (IG), we identified specific improvements needed to help ensure that security requirements are fully implemented. Evaluation results for these program elements are as follows.

Limitations Exist in GAO Information Technology Contingency Planning

GAO maintains an overall continuity program, which among other things, provides for the health and safety of GAO employees, contractors, and visitors, and ensures GAO will be able to maintain its operational capability in the event of a disaster or disruption. As a key element of this program, ISTS maintains a contingency plan that identifies and centralizes processes necessary to recover GAO Network services following a disruption that significantly degrades or disrupts network use.[6] Further, ISTS maintains detailed procedures for specific events, such as planned[7] and unscheduled power outages.[8]

These plans and procedures cover the GAO Network and all major applications (systems) located in the LOC at GAO Headquarters, and activating the plan may involve relocation of network operations to GAO's Alternate Computing Facility (ACF) located outside of Washington, D.C. However, as reported in the fiscal year 2011 evaluation, the ACF currently provides only limited disaster recovery capabilities and will require additional funding and executive support to build out the ACF infrastructure required to fully support GAO's mission-essential functions, should network operations become dependent on this facility.[9]

The ACF is equipped with servers to run a portion of applications to support mission-essential functions including the Document Management/Electronic Records Management System (DM/ERMS), General Counsel's case tracking system (GC Track), the Congressional Contact System, and My Locator. However, it is important to note that the data on these servers are not updated in real-time and in the event of an emergency, any changes made since the most recent update could be lost.

[6] *GAO Network IT Contingency Plan*, version 6.0 (August 2012).

[7] *Power Outage/Testing Checklist*, Version 1.1 (March 10, 2011).

[8] *Checklist Emergency LOC Shutdown*

[9] Mission Essential Functions (MEFs) are defined as a limited set of department- and agency-level government functions that must be continued after a disruption of normal activities.

Based on current procedures that include nightly incremental backup of data,[10] up to 24-hours' worth of data could be lost in an emergency.

In addition, although the ACF can provide "go-forward" e-mail services (no historical e-mail), ISTS does not yet have processes to migrate e-mails created through ACF operations back into LOC e-mail servers, should normal operations resume. This means that during a disaster or disruption, GAO personnel would not be able to access e-mails sent or received before the event. Further, once the event is over, any e-mails sent or received during the disruption may no longer be accessible. This could seriously impair communication with key stakeholders, including congressional staff and agency officials.

Other essential applications do not currently have servers at the ACF. These applications include the Asset Manager, the webTA System, the Job Information System, and the Engagement Results Phase. As a result, equipment would need to be procured or transferred to the ACF before any data could be loaded and restored. This would likely cause significant delays in recovering IT operations after an emergency.

In the event of a power outage or similar disruption, ISTS personnel would have approximately 15-20 minutes of emergency battery power to gracefully shut down approximately 300 servers in the GAO Headquarters LOC. According to ISTS personnel, the majority of federal agencies and private companies rely on a generator to extend that timeframe. This is consistent with NIST guidance that states organizations should provide a long-term alternate power supply for information systems that is capable of maintaining minimally-required operational capability in the event of an extended loss of the primary power source. ISTS personnel estimated that the cost for a generator was $2 million and deemed it to be cost-prohibitive. As a result, data on any server that is not shut down gracefully (i.e., employing log-off procedures that often require several minutes or more) is at risk of loss or corruption. That risk is significantly greater on evenings and weekends when the amount of ISTS staff physically on site is minimal.

We also noted that power circuits in the LOC are not redundant, which is not consistent with NIST guidance and industry best practices. For example, rows of servers are connected to a single Power Distribution Unit (PDU).[11] If the transformer within that PDU were to fail, the entire row of servers would lose power. Similarly, we observed that servers were plugged into the same circuit from a single PDU. If that circuit breaker were to trip or fail, those servers would lose power. To maintain

[10] An incremental backup captures files that were created or changed since the last backup. Incremental backups afford more efficient use of storage media, and backup times are reduced.

[11] A PDU is a device designed to transform raw power feeds into lower capacity power feeds and distribute that electricity to racks of computers and networking equipment located within the data center.

power redundancy, servers must be plugged into separate, independent power circuits.

Finally, ISTS informed us that they have not briefed members of the GAO Executive Committee on the specific risks posed by a power outage or similar disruption. We believe such briefings are an essential step in the Contingency Planning process.

Resource Challenges Exist in GAO's Information Security Program

Resource challenges in the Information Systems Security Group adversely impact GAO's ability to implement necessary upgrades identified by GAO managers and our prior work. For example, one area particularly affected is ISTS's ability to segregate responsibilities. Through interviews with ISTS personnel, we learned that staff have collateral duties that often pose competing priorities. For example, the Information System Security Officer (ISSO) is primarily responsible for ensuring implementation of system-level security controls and maintaining system documentation. However, the ISSO has also been assigned responsibility for audits and compliance. Similarly, engineering staff periodically have to perform monitoring duties or monitoring staff have to perform engineering duties. Further, the director frequently performs operational duties that take time away from management and strategic activities.

During our fiscal year 2011 evaluation, ISTS sometimes attributed competing resource needs as a cause for delayed correction of information security weakness. OMB and NIST guidance requires agencies to identify vulnerabilities, establish priorities, and assign staffing or financial resources required to resolve a weakness. We believe that estimating the resources needed to correct a weakness could aid in managing the overall remediation process.

Status of Prior Recommendations

During fiscal year 2012, to implement recommendations made in our FISMA evaluation for fiscal year 2011, ISTS took the following actions:

- Integrated an enterprise risk management program into its Information Technology Investment Committee governance and oversight process.
- Updated GAO's procedures for managing and tracking annual security awareness training and role based training to accurately report training compliance.
- Briefed senior management on the current ACF capabilities and a strategy for contingency operations at that site.

During fiscal year 2012, ISTS continued efforts to implement the one remaining 2011 FISMA recommendation that the CIO establish monitoring procedures that enhance accountability for, and management of, GAO's information security weakness remediation process by:

- Ensuring that business and system owners provide, and the Information Systems Security Group incorporates into the POA&M, timely updates that include current estimated completion dates for all open or delayed weaknesses; and
- Reconsidering the need to identify resources required to resolve a weakness, including funding or other nonfunding obstacles or challenges, such as staffing, that may adversely affect its remediation.

In addition, GAO continued efforts to implement the fiscal year 2009 FISMA recommendations to (1) develop policies and procedures that would meet the intent of a breach notification policy and plan as prescribed by OMB, and (2) establish a program to provide both initial and annual refresher privacy training to GAO's employees and managers. Implementing these two recommendations is dependent on finalizing a GAO security incident response directive and a GAO privacy rule and order, respectively. We commented on draft versions of these documents. However, as of February 7, 2013, these documents were not final.

Conclusions

Our prior year evaluations have shown that GAO has established an information security program that is generally consistent with federal requirements, guidance, and standards. Our fiscal year 2012 limited review reinforced our prior conclusion and identified areas for improvement in the contingency planning process. We also identified resource challenges that affect GAO's ability to implement security upgrades and strategies identified by GAO managers and the OIG.

It is essential to ongoing program effectiveness that GAO continually assess whether established processes and practices are operating as intended and make certain that changes in federal security requirements, guidance, and techniques are proactively incorporated into a formal, well-documented program. In addition, senior management involvement in determining how the organization assesses and mitigates information-system-related security risks will help to strengthen the agency's overall information security program.

Recommendations for Executive Action

To help strengthen GAO's overall information security program, we recommend that the CIO take the following two actions:

- Implement measures to increase the redundancy and availability of GAO mission-essential applications.
- Develop and provide, for GAO senior management consideration, a proposed strategy to ensure power redundancy to GAO servers and provide a long-term alternate power supply in the event of a power outage.

Agency Comments and Our Evaluation

The Inspector General provided GAO with a draft of this report for review and comment. (See attachment II.) GAO concurred with our recommendations. The agency also provided technical comments that we incorporated, as appropriate.

Actions taken in response to our recommendations are expected to be reported to my office within 60 days.

We are sending copies of this report to the other members of GAO's Executive Committee (Chief Operating Officer, Chief Administrative Officer/Chief Financial Officer, and General Counsel), GAO's Audit Advisory Committee, and other key managers. The report is also available on the GAO website at http://www.gao.gov/about/workforce/ig.html.

If you or your staff have any questions about this report, please contact me at (202) 512-5748 or trzeciaka@gao.gov. Contact points for GAO's Office of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this report were Douglas Carney and Cathy Helm, Deputy Inspector General.

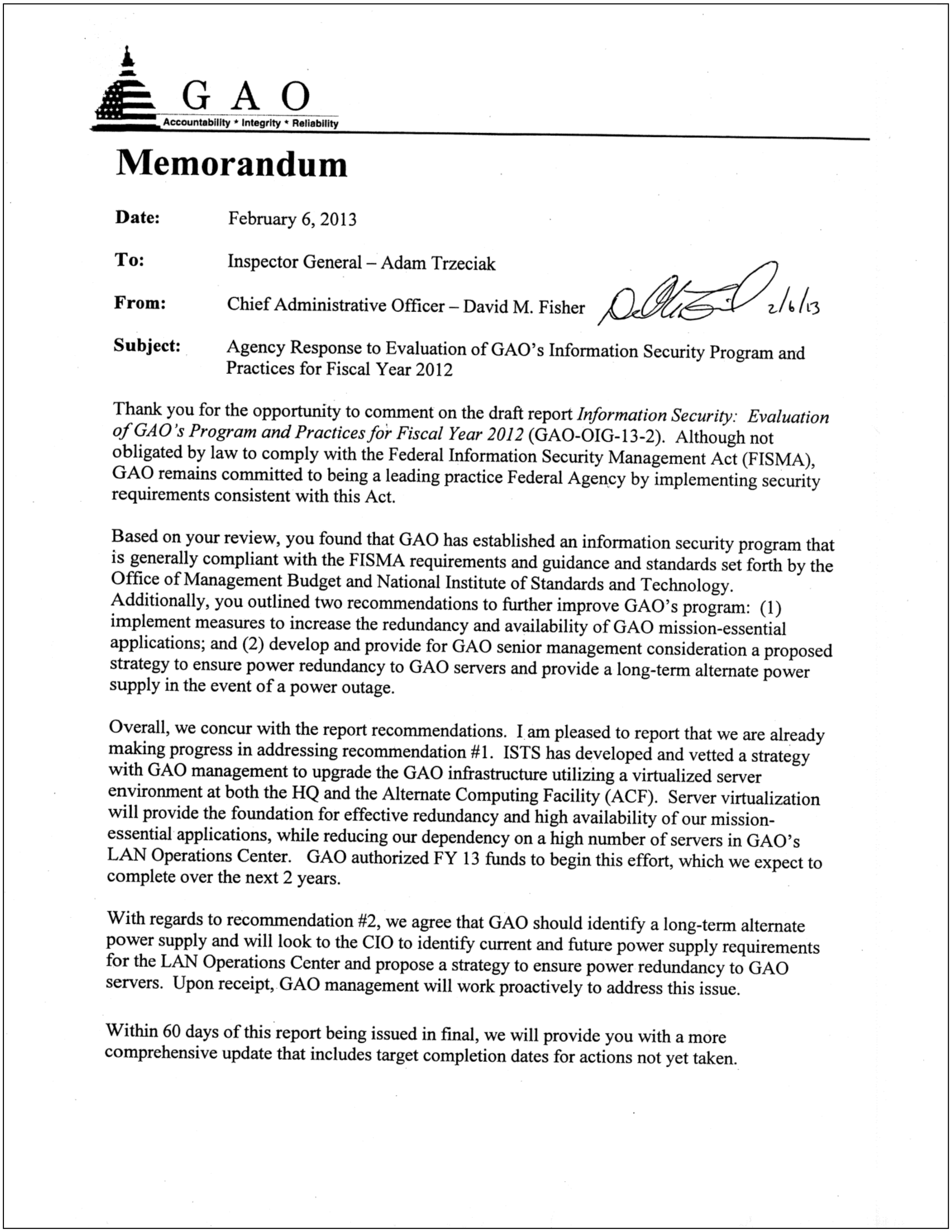
Attachment I

The following are the Department of Homeland Security's eighteen new fiscal year 2012 FISMA metrics for reporting by executive agency Inspectors General.[12]

2. CONFIGURATION MANAGEMENT	
2.1.8.	Software assessing (scanning) capabilities are fully implemented.
2.1.9.	Configuration-related vulnerabilities, including scan findings, have been remediated in a timely manner, as specified in Organization policy or standards.
2.1.10.	Patch management process is fully developed, as specified in Organization policy or standards.
3. IDENTITY AND ACCESS MANAGEMENT	
3.1.5.	Organization has adequately planned for implementation of PIV for logical access in accordance with government policies.
3.1.8.	Identifies all User and Non-User Accounts (refers to user accounts that are on a system. Examples of non-user accounts are accounts such as an IP that is set up for printing. Data user accounts are created to pull generic information from a database or a guest/anonymous account for generic login purposes that are not associated with a single user or a specific group of users)
4. INCIDENT RESPONSE AND REPORTING	
4.1.8.	There is sufficient incident monitoring and detection coverage in accordance with government policies.
5. RISK MANAGEMENT	
5.1.15.	Security authorization package contains Accreditation boundaries for Organization information systems defined in accordance with government policies.
6. SECURITY TRAINING	
6.1.6.	Training material for security awareness training does not contain appropriate content for the Organization.
7. PLAN OF ACTION & MILESTONES (POA&M)	
7.1.7.	Costs associated with remediating weaknesses are identified.
8. REMOTE ACCESS MANAGEMENT	
8.1.4.	Telecommuting policy is fully developed.
8.1.9.	Lost or stolen devices are disabled and appropriately reported.
8.1.10.	Remote access rules of behavior are adequate in accordance with government policies.
8.1.11.	Remote access user agreements are adequate in accordance with government policies.
9. CONTINGENCY PLANNING	
9.1.8.	After-action report that addresses issues identified during contingency/disaster recovery exercises.
9.1.9.	Systems that have alternate processing sites.
9.1.10.	Alternate processing sites are subject to the same risks as primary sites.
9.1.11.	Backups of information that are performed in a timely manner.
9.1.12.	Contingency planning that consider supply chain threats.

[12] U.S. Department of Homeland Security, *FY 2012 Inspector General Federal Information Security Management Act Reporting Metrics*, (March 6, 2012).

Attachment II



G A O

Accountability * Integrity * Reliability

Memorandum

Date: February 6, 2013

To: Inspector General – Adam Trzeciak

From: Chief Administrative Officer – David M. Fisher 2/6/13

Subject: Agency Response to Evaluation of GAO's Information Security Program and Practices for Fiscal Year 2012

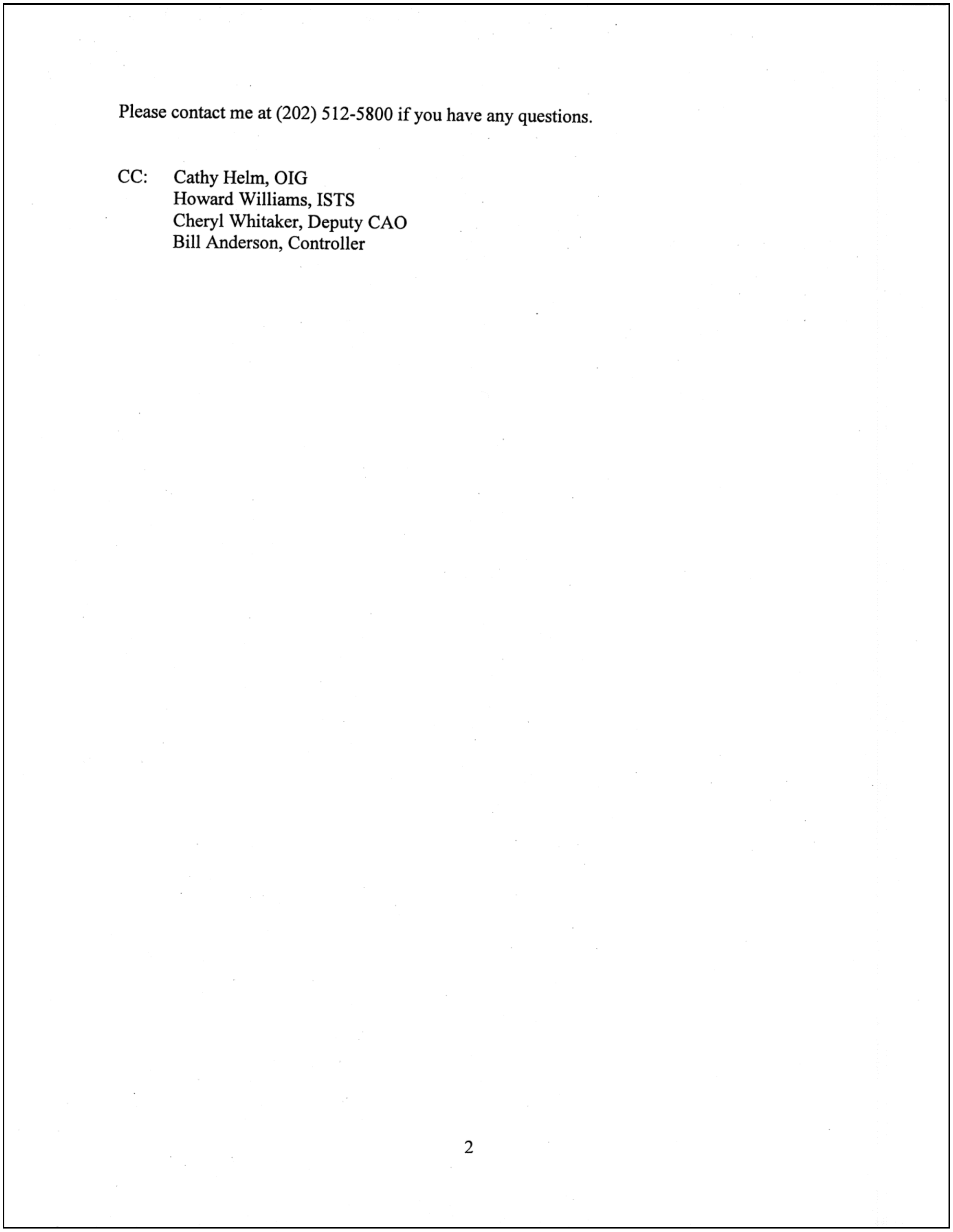
Thank you for the opportunity to comment on the draft report *Information Security: Evaluation of GAO's Program and Practices for Fiscal Year 2012* (GAO-OIG-13-2). Although not obligated by law to comply with the Federal Information Security Management Act (FISMA), GAO remains committed to being a leading practice Federal Agency by implementing security requirements consistent with this Act.

Based on your review, you found that GAO has established an information security program that is generally compliant with the FISMA requirements and guidance and standards set forth by the Office of Management Budget and National Institute of Standards and Technology. Additionally, you outlined two recommendations to further improve GAO's program: (1) implement measures to increase the redundancy and availability of GAO mission-essential applications; and (2) develop and provide for GAO senior management consideration a proposed strategy to ensure power redundancy to GAO servers and provide a long-term alternate power supply in the event of a power outage.

Overall, we concur with the report recommendations. I am pleased to report that we are already making progress in addressing recommendation #1. ISTS has developed and vetted a strategy with GAO management to upgrade the GAO infrastructure utilizing a virtualized server environment at both the HQ and the Alternate Computing Facility (ACF). Server virtualization will provide the foundation for effective redundancy and high availability of our mission-essential applications, while reducing our dependency on a high number of servers in GAO's LAN Operations Center. GAO authorized FY 13 funds to begin this effort, which we expect to complete over the next 2 years.

With regards to recommendation #2, we agree that GAO should identify a long-term alternate power supply and will look to the CIO to identify current and future power supply requirements for the LAN Operations Center and propose a strategy to ensure power redundancy to GAO servers. Upon receipt, GAO management will work proactively to address this issue.

Within 60 days of this report being issued in final, we will provide you with a more comprehensive update that includes target completion dates for actions not yet taken.



Please contact me at (202) 512-5800 if you have any questions.

CC: Cathy Helm, OIG
Howard Williams, ISTS
Cheryl Whitaker, Deputy CAO
Bill Anderson, Controller

(999827)

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

To report fraud, waste, and abuse in GAO's internal operations, do one of the following. (You may do so anonymously.)

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

Obtaining Copies of OIG Reports and Testimony

To obtain copies of OIG reports and testimony, go to GAO's Web site: www.gao.gov/about/workforce/ig.html.

Congressional Relations

Katherine Siggerud, Managing Director, siggerudk@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149, Washington, DC 20548