U.S. GOVERNMENT PRINTING OFFICE
OFFICE OF INSPECTOR GENERAL

ASSESSMENT REPORT
10-03

GPO's COMPLIANCE WITH THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT

January 12, 2010

U.S. GOVERNMENT PRINTING OFFICE
OFFICE OF INSPECTOR GENERAL

Date

January 12, 2010

To

Chief Information Officer

From

Assistant Inspector General for Audits and Inspections

Subject

GPO's Compliance with the Federal Information Security Management Act – Assessment Report
Report Number 10-03

The GPO Office of Inspector General (OIG) has completed an assessment of GPO's compliance with the Federal Information Security Management Act (FISMA). The overall objective of the assessment was to evaluate the design and effectiveness of controls over GPO's information security program, policies, and practices in accordance with FISMA. The scope included evaluating GPO's progress in complying with FISMA based on our initial baseline assessment conducted in Fiscal Year (FY) 2007[1]. As in FY 2007, the OIG engaged KPMG LLP (KPMG) to conduct the assessment. KPMG has substantial experience conducting FISMA assessments in the Federal government.

FISMA requires each Executive branch agency to develop, document, and implement an agency-wide program to provide information security for the information and information technology (IT) systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. While GPO is a Legislative branch agency, GPO also serves in effect, as a contractor to Executive branch agencies, and FISMA may apply to GPO. Nonetheless, GPO has chosen to comply with the principles of FISMA. The assessment was performed using the most recent applicable FISMA requirements and guidelines published by the Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST). The findings and recommendations are based on fieldwork conducted from July 31, 2008 through February 20, 2009.

---

[1] See OIG Report Number 07-09, *Final Report on GPO's Compliance with the Federal Information Security Management Act*, dated September 27, 2007.

Overall, while the assessment determined that GPO has made some progress in complying with FISMA, additional improvements are needed. Many of the weaknesses identified during the FY 2007 baseline assessment still exist. GPO has made progress in the following areas including:

- Implementation of a methodology for developing an inventory of IT systems.
- Categorization of its major systems in accordance with the NIST standard[2] required by FISMA.
- Development of a process for certifying and accrediting its major applications and general support systems in accordance with the NIST standard required by FISMA.
- Implementation of certain controls to enhance the protection of personally identifiable information (PII).

As a result of the assessment, twenty-one (21) recommendations are being made in the following areas in order for GPO to further comply with FISMA:

- System inventory (while a system inventory methodology has been developed, a comprehensive inventory has not been produced);
- Security control testing;
- Security Plan of Action and Milestone (POA&M) process;
- Contingency Planning;
- Security Incident Reporting;
- Privacy and PII Processes and Controls;
- Systems Security Plans;
- Security Risk Assessments;
- Certification and Accreditation (C&A) of major GPO systems; and
- System Security Configuration and Patch Management processes.

The KPMG report (Enclosure) provides a summary as well as the detailed findings and recommendations from the assessment. Appendix A of this (OIG) report contains GPO management's response. We consider the actions taken or propose by management to be responsive to each of the report's recommendations. Recommendation number 7 states that Plans of Actions and Milestones (POA&Ms) should continue to be reviewed periodically by the GPO OIG. We agree with this recommendation and will conduct our

---

[2] NIST requires that agencies categorize their information and information systems based on the potential impact certain events would have on the information and information systems needed by to accomplish the agency's assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. Security categories are to be used in conjunction with vulnerability and threat information in assessing the risk to an organization.

initial review during the first quarter of FY 2010. Each of the 21 recommendations is considered resolved and will remain open pending follow-up by the OIG. The status of each recommendation upon issuance of this report is included in Appendix B. The final report distribution is in Appendix C.

If you have any questions concerning the report or the assessment process, please contact Mr. Brent Melson, Deputy Assistant Inspector General for Audits and Inspections at (202) 512-2037, or myself at (202) 512-2009.

Kevin J. Carson
Assistant Inspector General for Audits and Inspections

Enclosure

cc:
Deputy Public Printer
Acting Chief of Staff
Acting General Counsel
Chief Technology Officer
Chief Management Officer
Chief Information Security Officer

Enclosure

United States Government Printing Office
Office of Inspector General

Federal Information Security Management Act (FISMA) Evaluation

Final Report

October 22, 2009

GOVERNMENT PRINTING OFFICE

FEDERAL INFORMATION SECURITY MANAGEMENT ACT (FISMA) EVALUATION

FINAL REPORT

October 22, 2009

Table of Contents

EXECUTIVE SUMMARY

The Federal Information Security Management Act (FISMA) requires that each Executive branch agency develop, document, and implement an agency-wide information security program to protect information and information systems that support the operations and assets of the agency, including those systems provided or managed by another agency or contractor. FISMA further requires that each Executive branch agency perform an annual review of the design and effectiveness its information security program.

Although the Government Printing Office (GPO, the Agency) is a Legislative branch agency and is therefore not required by law to adhere to FISMA requirements, GPO has recognized the need to be FISMA compliant due to the services that GPO provides to other entities, including Executive branch agencies. As a result, the GPO Office of Inspector General (OIG) contracted for an evaluation of the Agency's FISMA compliance efforts, and the resulting report was issued in fiscal year 2007. As a follow up to that effort, the GPO OIG again contracted for an evaluation of the Agency's FISMA compliance and to evaluate GPO's efforts to address issues identified in the fiscal year 2007 report, and the results are contained in this report.

The overall objective of the FISMA evaluation was to assess the design and effectiveness of the controls over GPO's information security program, policies, and practices. The scope of the evaluation included the review of the information technology (IT) security program managed by the GPO Office of the Chief Information Officer (OCIO) under the direction of the Chief Information Security Officer (CISO). The scope specifically included processes and controls GPO has in place to protect sensitive information, such as device security configurations and personally identifiable information (PII)[1]. The evaluation approach included reviewing documentation and interviewing GPO personnel responsible for the security and administration of information and IT resources. Fieldwork was conducted from July 31, 2008, through February 20, 2009 at the GPO Headquarters in Washington, DC.

Office of Management and Budget (OMB) Memorandum M-08-21, "Fiscal Year 2008 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management" was used as the framework for performing and reporting the

[1] Office of Management and Budget Memorandum 07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information" defines "personally identifiable information" as information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

results of this FISMA evaluation. Additionally, OMB Memoranda M-07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information" and M-08-09, "New FISMA Privacy Reporting Requirements for Fiscal Year 2008" were used as guidance for assessing and reporting GPO's efforts to ensure the privacy of PII. Guidance was also obtained from other Federal laws, guidelines, and requirements pertaining to the protection of Federal information resources. Because GPO is not an Executive branch agency, these requirements and guidelines are not considered authoritative, rather they are best practices.

We determined that GPO made progress in complying with FISMA, but we also found that additional improvements are needed, and that many of the weaknesses identified in the FY 2007 evaluation report still exist. In summary, GPO should:

- Develop a more accurate and comprehensive inventory of the agency's major applications, minor applications, and general support systems.

- Implement a process to review and test the effectiveness of the security controls of its major systems on a periodic basis.

- Develop a comprehensive and centralized process for tracking and monitoring the status and remediation of all known security weaknesses.

- Ensure that a complete and comprehensive process for identifying, reporting, and resolving computer security incidents is in place.

- Develop a complete and comprehensive process for granting major application and general support systems the authority to operate within GPO's IT infrastructure. This process should ensure that the risks posed to each system are assessed, supporting security controls are properly designed and implemented, and contingency plans are created and tested at least annually.

- Ensure that the necessary safeguards are in place to enable the privacy and protection of PII.

- Complete the implementation of processes and controls to enhance the system security configuration management and patch management processes.

Given the sensitivity of the issues, the detailed findings and recommendations have been provided to GPO management under separate cover. Further, we have marked the separate detailed findings and recommendations as "Non-Public – For Internal Use Only", and the document has a limited distribution. Recipients of the detailed findings and recommendations are expected to follow the established policies and procedures for

managing and safeguarding the non-public information, including restricting the distribution of the non-public information in whole or in part.

BACKGROUND

FISMA was signed into law on December 17, 2002, as Title III, "Information Security," of the E-Government Act of 2003. FISMA permanently reauthorized the framework established by the Government Information Security Reform Act (GISRA), which expired in November 2002. FISMA requires that each Executive branch agency develop, document, and implement an agency-wide information security program to protect information and information systems that support the operations and assets of the agency, including those systems provided or managed by another agency or contractor. FISMA further requires that each Executive branch agency perform an annual review of the design and effectiveness its information security program.

Although GPO is a Legislative branch agency and is therefore not required by law to adhere to FISMA requirements, GPO has recognized the need to be FISMA compliant due to the services that GPO provides to other entities, including Executive branch agencies. As a result, the GPO OIG contracted with KPMG LLP (KPMG) to perform an evaluation of the Agency's FISMA compliance efforts, and the resulting report was issued in fiscal year 2007. As a follow up to that effort, the GPO OIG again engaged KPMG to evaluate the Agency's FISMA compliance and to evaluate GPO's efforts to address issues identified in the fiscal year 2007 report, and the results are contained in this report.

OMB Memorandum M-08-21, "Fiscal Year 2008 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management" was used as the framework for performing and reporting the results of this FISMA evaluation. Additionally, OMB Memoranda M-07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information" and M-08-09, "New FISMA Privacy Reporting Requirements for Fiscal Year 2008" were used as guidance for assessing and reporting GPO's efforts to ensure the privacy of PII. Guidance was also obtained from other Federal laws, guidelines, and requirements pertaining to the protection of Federal information resources. Because GPO is not an Executive branch agency, these requirements and guidelines are not considered authoritative, rather they are best practices. Laws, requirements, and guidelines used in the course of this evaluation included:

- The E-Government Act of 2002, Public Law 107-347, enacted on December 17, 2002

- OMB Circular A-130, entitled "Management of Federal Information Resources", as revised on November 30, 2000

- OMB M-07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information"

- OMB M-08-09, "New FISMA Privacy Reporting Requirements for Fiscal Year 2008"

- National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) 199, "Standards for Security Categorization of Federal Information and Information Systems"

- NIST FIPS 200, "Minimum Security Requirements for Federal Information and Information Systems"

- NIST Special Publication (SP) 800-12, "An Introduction to Computer Security: The NIST Handbook"

- NIST SP 800-18, "Guide for Developing Security Plans for Federal Information Systems"

- NIST SP 800-30, "Risk Management Guide for Information Technology"

- NIST SP 800-34, "Contingency Planning Guide for Information Technology Systems"

- NIST SP 800-37, "Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems," enacted May 2004

- NIST SP 800-61, "Computer Security Incident Handling Guide"

- NIST SP 800-70, "The NIST Security Configuration Checklists Program"

During this evaluation we also applied relevant GPO-specific requirements and guidance.

Our evaluation procedures were designed to comply with applicable auditing standards and guidelines, specifically the Generally Accepted Government Auditing Standards (GAGAS).

OBJECTIVE

The overall objective of this evaluation was to evaluate the design and effectiveness of controls over GPO's information security program by assessing the risk for each component of the program. The specific objectives of the evaluation included:

- Assessing GPO's process for developing a systems inventory that included major and minor applications and general support systems. This portion of the evaluation also included assessing GPO's process for identifying and recording both system interfaces and contractor operated systems.

- Determining if a process was in place to ensure that all GPO systems have been categorized according to NIST FIPS 199, "Standards for Security Categorization of Federal Information and Information Systems".

- Assessing GPO's process for certifying and accrediting major applications and general support systems. This portion of the evaluation included reviewing risk assessments, security plans, security evaluations, and contingency plans for a sample of mission critical GPO systems to assess compliance against NIST information security guidance as required by FISMA.

- Assessing GPO's process for tracking the remediation of known IT security weaknesses (i.e. through the use of a Plan of Action and Milestones (POA&M) process).

- Assessing GPO's process for ensuring the proper implementation, maintenance, and modification of security controls for select Agency systems.

- Assessing GPO's process for identifying, reporting, and responding to computer security incidents.

- Determining whether GPO has implemented a security awareness training program for employees and contractors.

- Assessing GPO's compliance with FISMA and OMB requirements for ensuring the privacy of PII.

SCOPE

The scope of the evaluation included the review of the information technology (IT) security program managed by the GPO Office of the Chief Information Officer (OCIO) under the direction of the Chief Information Security Officer (CISO). The approach included evaluating documentation and interviewing GPO personnel responsible for the security and administration of information and IT resources. Fieldwork was conducted from July 31, 2008, through February 20, 2009 at the GPO Headquarters in Washington, DC.

AUDIT OBSERVATIONS AND RECOMMENDATIONS

We determined that GPO made progress in complying with FISMA. Specifically, we noted the following positive efforts:

- GPO has recognized the importance of FISMA and has a commitment to complying with the law. For example, GPO has: 1) implemented a methodology for developing an inventory of IT systems, 2) classified its major systems in accordance with FIPS 199, 3) developed a process for certifying and accrediting its major applications and general support systems according to OMB NIST standards, and 4) implemented certain controls to enhance the protection of PII.

- The GPO Information Technology and Systems (IT&S) group has implemented various tools, including a vulnerability scanner and security monitoring service, to routinely identify, assess, and remediate network security weaknesses.

Despite these accomplishments, in order to progress further towards becoming FISMA compliant, GPO needs to improve in several areas, which are noted below.

System Inventory. GPO's process for identifying, recording, and maintaining its system inventory has not produced a comprehensive and current system inventory, including major systems (core operating systems and general support systems), as well as the supporting hardware and peripherals. FISMA requires the head of each agency to develop and maintain an inventory of major information systems operated by or under the control of such agency (included in this requirement are national security systems, but GPO does not have any such systems). GPO has a process for recording and maintaining the Agency's system inventory, but the process is manually intensive, and with current competing priorities GPO has been unable to maintain a comprehensive and complete inventory. This issue was also identified in the fiscal year 2007 GPO FISMA evaluation report, and although GPO has taken some corrective actions, the weakness remains.

Without a complete and comprehensive system inventory, GPO is at elevated risk of not having an accurate accounting of its IT assets, including system interfaces and underlying data elements. Consequently, potential security risks may not be properly identified and mitigated, leading to negative impacts on operations. Furthermore, administrative functions such as IT resource management, capital planning, and strategic planning could be negatively impacted.

Recommendations

1) GPO should enhance the existing system inventory to ensure it contains all major Agency systems and supporting interfaces and peripheral equipment.

2) The results of the periodic network and system scanning activities should be used to assist in reconciling and validating the inventory listings.

3) To support Recommendation #1, detailed procedures should be developed to describe the process the business units should use to include systems in the Agency inventory.

Security Control Testing. Although GPO performed routine network vulnerability assessments during fiscal year 2008, periodic security control assessments were not performed for several key systems. FISMA requires Federal agencies to provide information security for the information and information systems that support the operations and assets under their control, including periodic testing. Further, GPO's "Information Technology Security Program Statement of Policy" (GPO Directive 825.33A) requires senior GPO officials to periodically test and evaluate information security controls. Similar weaknesses were identified in the fiscal year 2007 FISMA evaluation report, and although GPO has taken some corrective actions, such as performing network testing, additional efforts are needed.

GPO management recognizes the need to complete periodic review of security controls for major systems, and as noted above, performs such testing on the network. However, competing priorities have limited GPO's abilities to complete all necessary reviews of all key systems. Without periodic reviews of security controls for key systems, new threats and vulnerabilities may not be identified and mitigated in a timely manner, thus elevating the risk of loss, damage, or theft of valuable information and/or resources.

Recommendation

4) GPO should take action to fully implement the FISMA and Agency security requirement to perform periodic security reviews for key systems. The reviews should be conducted in accordance with NIST SP 800-53A, "Guide for Assessing Security Controls in Federal Information Systems". Specifically, the security reviews should document scope of the reviews, the procedures to be performed, and the results of the reviews. Further, the system certification and accreditation (C&A) packages (e.g., risk assessments, security plans) should be updated as needed based on the reviews.

Security Plan of Action and Milestone (POA&M) Process. The process used by GPO to track and monitor IT security weaknesses does not meet OMB and FISMA requirements for developing security POA&Ms. OMB Memorandum M-08-21, "Fiscal Year 2008 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management", guides that security POA&Ms must include all security weaknesses found during any other review done by, for, or on behalf of the agency. Similar weaknesses were identified in the fiscal year 2007 FISMA evaluation

report, but due to competing staff priorities, GPO's IT Security function was unable to perform quarterly reviews of POA&M activities during Fiscal Year 2008. However, a quarterly review process was implemented during the fourth quarter of fiscal year 2008.

Without periodic updates and reviews of POA&M activities, the risk is elevated that GPO may be unaware of the current status of security-related corrective actions. As a result, delays in the implementation of corrective actions may not be appropriately identified and resolved in a timely manner. Additionally, GPO is at risk that resources needed to mitigate the weaknesses may not be sufficiently planned.

Recommendations

5) GPO's POA&M process should include procedures for tracking and monitoring the status of system-specific weaknesses and the development of executive-level summaries for the POA&Ms.

6) POA&Ms should be periodically reviewed by the OCIO, at a minimum, on a quarterly basis. The OCIO should utilize the quarterly review of POA&Ms to assess the timeliness of corrective actions and the appropriateness of resources applied to the corrective actions. The periodic reviews should entail:

- Descriptions of the identified security weaknesses, including severity
- Methods used to identify the security weaknesses
- Identification of the GPO function responsible for resolving the weaknesses
- Estimated resources needed to mitigate the weaknesses
- Planned milestones and completion dates
- Status of corrective actions

7) POA&Ms should continue to be reviewed periodically by the GPO OIG to help ensure independent verification and validation of identified weaknesses and planned corrective actions.

8) The POA&M process should be coordinated with GPO's IT capital planning efforts to help ensure that security costs are linked to actual system security performance.

Contingency Planning. System contingency plans have not been completed and tested for several key GPO systems. Similar weaknesses were identified in the fiscal year 2007 FISMA evaluation report, and GPO has taken some corrective actions. For example, a Business Impact Analysis (BIA) was completed during the first quarter of fiscal year 2008, and the results are being used to finalize contingency planning efforts for GPO's general support system. System-specific contingency plans will then be developed to complement the general support system contingency plan.

FISMA requires each agency to develop plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency. Further, GPO Publication 825.33, "Information Technology Security Program Statement of Policy", requires the Agency to define, document, and manage the contingency planning process, including training and testing, to provide IT systems with adequate continuity of operations upon disruption of normal operations. GPO recognizes the need to complete contingency plans for key systems, but competing priorities have limited the Agency's abilities to complete all necessary contingency plans.

Without effective contingency planning, which includes periodic testing of the plan's accuracy and reliability, GPO may be unable to access critical information and resources and perform mission critical business functions during an extended outage and/or disaster. Further, key parties and responsible individuals may not fully understand their roles and responsibilities during the execution of the plan. As a result, GPO may be unable to resume operations in an efficient and effective manner and meet its customers' demands for products and services.

Recommendations

9) GPO should continue the development of its business resumption and contingency planning efforts in accordance with NIST SP 800-34, "Contingency Planning Guide for Information Technology Systems" to enable appropriate contingency support to mission critical systems and business functions.

10) Upon the completion of contingency plans for each of the GPO's major systems, the Agency should provide training to appropriate personnel, perform periodic testing of the plans, and update the plans based on the results of the testing. Test plans should address system recovery from backup media on an alternate platform, coordination among recovery teams, internal and external connectivity, performance of systems when using alternate equipment, restoration of normal operations, and notification procedures.

Security Incident Reporting. The GPO "Computer Security Incident Response Team (CSIRT) Framework and Procedures" do not address all of the elements outlined in NIST SP 800-61, "Computer Security Incident Handling Guide." Additionally, GPO has not developed specific procedures for reporting incidents of PII exposures, as required by OMB Memo M-07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information." Further, FISMA requires agencies to sufficiently detect, report, and respond to security incidents. Similar weaknesses were identified in the fiscal year 2007 FISMA evaluation report.

GPO recognizes the need to have more complete incident reporting processes and guidelines, but competing priorities have limited the Agency's abilities to do so. An effective incident response capability is necessary to quickly detect security incidents, minimize loss and destruction, mitigate the weaknesses, and restore computing services. An inadequate incident response capability could delay the detection, mitigation, and restoration of IT and business processing in the event of an attack.

Recommendation

11) GPO should develop a complete and comprehensive process for identifying, reporting, and resolving computer security incidents, as well as developing a PII breach notification policy covering both electronic and paper breaches of PII.

Privacy and PII Processes and Controls. GPO has not fully implemented controls necessary to identify, protect, and limit the use of PII. For example, Privacy Impact Assessments (PIAs) have not been completed for all key GPO systems. FISMA, consistent with the Privacy Act of 1974, requires each agency to establish rules of conduct for persons involved with PII, establish safeguards for PII, and maintain accurate, relevant, timely and complete PII information. Similar weaknesses were identified in the fiscal year 2007 FISMA evaluation report. As with FISMA, as a Legislative branch agency GPO is not required by law to adhere to Privacy Act requirements, but the Agency has recognized the Privacy Act as a best practice so we include it as criteria for this evaluation.

GPO has not designated an official responsible for managing and monitoring the Agency's privacy compliance efforts (e.g., Chief Privacy Officer). As a result, privacy requirements have not been adequately identified and subsequently communicated to other responsible program officials (e.g. OCIO). Additionally, competing priorities have prevented the completion of PIAs. GPO did partially deploy a full disk encryption process during fiscal year 2008, which can effectively facilitate the protection of PII, but not all Agency mobile devices have been equipped yet with the encryption software.

Without the proper identification, protection, and limitation of the use of PII, GPO systems and devices containing PII may be susceptible to unidentified threats and security weaknesses. Additionally, the use of PII may not be adequately restricted, thereby leading to the improper dissemination of sensitive information. As a result, unauthorized persons may gain access to valuable resources and sensitive information.

Recommendations

12) GPO should designate a responsible official (e.g., Chief Privacy Officer) for managing and monitoring the Agency's privacy compliance efforts. The designated

official should participate in GPO's information privacy compliance activities, evaluate the ramifications for privacy of legislative, regulatory, and other policy proposals, and participate in assessing the impact of technology on PII.

13) To comply with requirements of OMB Memorandum M-07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information", we recommend that GPO develop a policy concerning the responsibilities of individuals authorized to access PII and implement: 1) a plan to eliminate the unnecessary use of PII, including the identification of suitable alternatives, and 2) a policy requiring users with authorized access to PII to reconfirm in writing the acceptance of their responsibilities to protect PII from misuse and exposure on an annual basis.

14) GPO should continue with plans to encrypt data on all portable devices.

15) GPO should complete PIAs for key systems.

System Security Plans. System security plans address the controls necessary to adequately mitigate identified security risks to an acceptable level, and are key components of the system C&A process. However, system security plans have not been developed for all of GPO's major systems in accordance with FISMA and NIST SP 800-18, "Guide for Developing Security Plans for Federal Information Systems." Specifically, FISMA requires agencies to document plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate. Further, NIST SP 800-18 guides that all information systems must be covered by a system security plan. Similar weaknesses were identified in the fiscal year 2007 FISMA evaluation report.

GPO recognizes the need to have documented system security plans for all major systems, and has developed a template based upon NIST SP 800-18 and SP 800-53 guidelines to aid the development of the plans. However, competing priorities have limited the Agency's abilities to do so. Without complete and comprehensive system security plans that document planning activities undertaken by GPO to protect IT resources, the risk is elevated for: 1) not effectively communicating the importance of system security to users, and 2) not providing a basis by which management can ensure the effectiveness of security measures. System security plans allow GPO to have complete and comprehensive plans that provide an overview of the security requirements and describes the controls in place or planned for meeting those requirements.

Recommendation

16) GPO should ensure that security plans are completed for each major system. The security plans should completely, accurately, and comprehensively address all required

elements of NIST SP 800-18, "Guide for Developing Security Plans for Federal Information Systems."

Security Risk Assessments. Prior to the development of the system security plan, a security risk assessment must first be performed for each major application or general support system to determine the risks posed to each respective system. Once finalized, the output of the risk assessment should be used to determine the appropriate level of controls needed to adequately protect each information system from the threats identified. These controls should be adequately and completely documented in the system security plan. Despite the importance of security risk assessments, GPO has not performed risk assessments for all key systems. A similar weakness was identified in the fiscal year 2007 FISMA evaluation report.

FISMA requires each agency to conduct periodic assessments of the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency and policies and procedures that are based on the risk assessments. Further, NIST SP 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems" guides that risk assessments are needed to influence the development of the security controls for information systems and generate much of the information needed for the associated system security plans.

GPO recognizes the need to have documented risk assessments, and has developed a system questionnaire template that maps to NIST SP 800-53 to facilitate the performance of risk assessments. The questionnaire appears adequate to facilitate completion of the risk assessments, but competing priorities have limited the Agency's abilities to complete risk assessments for all key systems. Without the performance of a comprehensive documented risk assessment for each key system, GPO may not successfully identify the security risks posed by the operation of the system. As a result, GPO may not adequately monitor and mitigate risks to a level deemed acceptable by Agency management.

Recommendations

17) GPO should complete risk assessments for its major applications and systems in accordance with the guidance outlined in NIST SP 800-30, "Risk Management Guide for Information Technology Systems." Further, system owners should accept any residual risk associated with the assessments. The acceptance of residual risk should be reviewed and formally documented by the OCIO.

18) Upon the completion of the risk assessments, GPO should determine the appropriate levels of controls that are needed to adequately protect each information system from the threats identified. The controls should be adequately and completely documented in the

related system security plans per the guidance outlined in the NIST SP 800-18, "Guide for Developing Security Plans for Federal Information Systems."

System C&A Process. Several key GPO systems did not receive C&As prior to implementation into the production environment. Interim Authorities to Operate (IATOs) were granted for several systems rather than the full C&A, and although an IATO does grant a limited authority to operate it does not constitute the FISMA-required full C&A.

GPO Publication 825.33, "Information Technology Security Program Statement of Policy", requires systems to undergo a C&A before they process any data. Additionally, systems must be re-accredited at least every 3 years, or when a significant change is made to the configuration of the system. Further, NIST SP 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems" guides that the successful completion of the security C&A process provides agency officials with the necessary confidence that the information system has adequate security controls, that any vulnerabilities in the system have been considered in the risk-based decision to authorize processing, and that appropriate plans and funds have been identified to correct any deficiencies in the information system.

GPO recognizes the need to have complete C&A packages for Agency systems, but competing priorities have limited the Agency's abilities to do so. Without full C&As for GPO major applications and systems, the Agency may not be sufficiently identifying and mitigating the security risks posed by the introduction of new or revised applications and systems into the production environment. As a result, applications and systems may operate in the production environment without appropriate controls or management oversight.

Recommendations

19) GPO should continue its efforts to complete the C&A of its major applications and systems in accordance with NIST SP 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems." These efforts should include the development and maintenance of documentation used in the certification process and the security accreditation decision (e.g. risk assessments, system security plans, and contingency plans).

20) GPO should maintain a schedule to track C&A life cycle activities of each major application and general support system. This schedule should include:

- The stage of the C&A process for each system (i.e., IATO or full authority to operate) and the expected date of authorization.

- The completion date or expected completion date of each component of the certification and accreditation process, including system security plans, contingency plans, and risk assessments.

- If authorized, the schedule should also include the projected date of re-certification.

The system owner's name and contact information should be identified for each system.

System Security Configuration Management and Patch Management Processes. GPO has not fully implemented controls to ensure the security configuration of systems, notably the Microsoft Windows operating system, Microsoft Internet Information Server (IIS), and Oracle database management system. This condition has been reported in prior GPO financial statement audits and GPO Office of Inspector General (OIG) reports, including the 2007 FISMA evaluation. In response to prior year findings, GPO began implementing the Configuresoft Security Update Manager (SUM) software to more effectively monitor the security configurations for key systems and the software patch management process. However, the tool has not been fully implemented.

FISMA requires each agency to ensure compliance with minimally acceptable system configuration requirements. GPO recognizes the need to improve controls over the system security configuration and patch management processes, and the Agency has partially implemented the Configuresoft SUM tool. However, competing resources have limited the full implementation of the tool.

As a complement to the use of the Configuresoft SUM, GPO relies on periodic vulnerability scans to validate the security configuration for key systems. Although the use of a vulnerability scanning process may identify non compliance with system security configurations, the process does not provide a complete assessment of the security configurations. For example, system and device configurations, such as audit settings, file permissions, account permissions, and administrator/root usage may not be fully assessed for compliance with GPO's security configuration baseline. Further, the vulnerability assessment process does not provide a real time assessment of security configurations, which the Configuresoft SUM tool provides.

Recommendations

21) GPO should continue with plans to implement the Configuresoft SUM tool to more effectively manage real time system security configurations and the patch management process.

Enclosure

United States Government Printing Office
Office of Inspector General

Federal Information Security Management Act (FISMA) Evaluation

Final Report

Detailed Findings and Recommendations

October 22, 2009

Detailed Findings and Recommendations

The findings identified in this Appendix were noted during the FISMA evaluation. Each finding includes the condition, cause, criteria, effect, and a recommendation for GPO consideration. Because GPO is not an executive branch agency, the Federal criteria cited in the findings (other than GPO-specific criteria) is not considered authoritative, rather they are best practices. Note that elements for many of these findings were also identified in the fiscal year 2007 GPO FISMA evaluation report.

Finding 2008-FISMA-01: System Inventory

Condition

GPO's process for identifying, recording, and maintaining its system inventory has not produced a comprehensive and current system inventory, including major systems (core operating systems and general support systems), as well as the supporting hardware and peripherals. This issue was also identified in the fiscal year 2007 GPO FISMA evaluation report, and although GPO has taken some corrective actions, the weakness remains.

Criteria

FISMA requires:

> "The head of each agency shall develop and maintain an inventory of major information systems (including major national security systems) operated by or under the control of such agency.
>
> The identification of information systems in an inventory under this subsection shall include an identification of the interfaces between each such system and all other systems or networks, including those not operated by or under the control of the agency. Such an inventory shall be:
>
> - Updated at least annually
> - Made available to the Comptroller General
> - Used to support information resources management"

Cause

In response to the fiscal year 2007 FISMA evaluation report, GPO enhanced its process for recording and maintaining the Agency's system inventory. However, the process is

still manually intensive, and with current competing priorities GPO has been unable to maintain a comprehensive and complete inventory.

Effect

Without a complete and comprehensive system inventory, GPO is at elevated risk of not having an accurate accounting of its IT assets, including system interfaces and underlying data elements. Consequently, potential security risks may not be properly identified and mitigated, leading to negative impacts on operations. Furthermore, administrative functions such as IT resource management, capital planning, and strategic planning could be negatively impacted.

Recommendations

1) GPO should enhance the existing system inventory to ensure it contains all major Agency systems and supporting interfaces and peripheral equipment. The inventory should contain systems operated by or under the control of GPO, as well as those operated by third party contractors or other agencies on behalf of GPO. To accomplish this effort GPO should have each Agency business unit update their respective inventories and submit them to the Office of the Chief Information Officer (OCIO). The OCIO should then consolidate the listings, and going forward should also periodically reconcile the inventory with the business units through the use of a questionnaire.

2) The results of the periodic network and system scanning activities should be conducted to assist in reconciling and validating the inventory listings.

3) To support Recommendation #1, detailed procedures should be developed to describe the process the business units should use to include systems in the Agency inventory. The procedures should include a detailed definition of systems, system boundaries, and system classifications. Further, the procedures, and the resulting inventory, should be linked to the Agency's IT resource management, capital planning, and strategic planning efforts.

Finding 2008-FISMA-02: Security Control Testing

Condition

Although GPO performed routine network vulnerability assessments during fiscal year 2008, periodic security control assessments were not performed for three of GPO's major systems (GPO Access, GPO Web Hosting, and the Passport Printing and Production System (PPPS)). Similar weaknesses were identified in the fiscal year 2007 FISMA evaluation report, and although GPO has taken some corrective actions, such as performing network testing, additional efforts are needed.

Criteria

FISMA requires:

> "The head of each agency shall ensure that senior agency officials provide information security for the information and information systems that support the operations and assets under their control, including through periodically testing and evaluating information security controls and techniques to ensure that they are effectively implemented.
>
> Each agency shall develop, document, and implement an agency-wide information security program, approved by the Director, to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source, that includes periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, to be performed with a frequency depending on risk, but no less than annually."

GPO "Information Technology Security Program Statement of Policy" (GPO Directive 825.33A) requires senior GPO officials to periodically test and evaluate information security controls.

Cause

Competing priorities have limited GPO's abilities to complete necessary reviews for all key systems.

Effect

Without periodic reviews of security controls for key systems, new threats and vulnerabilities may not be identified and mitigated in a timely manner, thus elevating the risk of loss, damage, or theft of valuable information and/or resources.

Recommendation

4) GPO should take action to fully implement the FISMA and Agency security requirement to perform periodic security reviews for key systems. The reviews should be conducted in accordance with NIST Special Publication (SP) 800-53A, "Guide for Assessing Security Controls in Federal Information Systems". Specifically, the security reviews should document scope of the reviews, the procedures to be performed, and the results of the reviews. Further, the system certification and accreditation (C&A) packages (e.g., risk assessments, security plans) should be updated as needed based on the reviews.

Finding 2008-FISMA-03: POA&M Process

Condition

The process used by GPO to track and monitor IT security weaknesses does not meet OMB and FISMA requirements for developing security POA&Ms. Specifically, GPO has not implemented procedures to review and update POA&Ms on a quarterly basis. Similar weaknesses were identified in the fiscal year 2007 FISMA evaluation report.

Criteria

OMB Memorandum M-08-21, "Fiscal Year 2008 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management", guides:

> "POA&Ms must include all security weaknesses found during any other review done by, for, or on behalf of the agency, including GAO audits, financial system audits, and critical infrastructure vulnerability assessments. These plans should be the authoritative agency-wide management tool, inclusive of all evaluations.
>
> A POA&M, also referred to as a corrective action plan, is a tool that identifies tasks that need to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the task, and scheduled completion dates for the milestones. The purpose of the POA&M is to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and systems.
>
> Program officials and contractors report progress on security weakness remediation to the CIO on a regular basis (at least quarterly) and the Agency CIO centrally tracks, maintains, and reviews POA&M activities on at least a quarterly basis."

Cause

Due to competing staff priorities, GPO's IT Security function was unable to perform quarterly reviews of POA&M activities during fiscal year 2008 and address all weaknesses identified in the fiscal year 2007 FISMA evaluation report. However, a quarterly review process was implemented during the fourth quarter of fiscal year 2008.

Effect

Without periodic updates and reviews of POA&M activities, the risk is elevated that GPO may be unaware of the current status of security-related corrective actions. As a result, delays in the implementation of corrective actions may not be appropriately identified

and resolved in a timely manner. Additionally, GPO is at risk that resources needed to mitigate the weaknesses may not be sufficiently planned.

Recommendations

5) GPO's POA&M process should include procedures for tracking and monitoring the status of system-specific weaknesses and the development of executive-level summaries for the POA&Ms.

6) POA&Ms should be periodically reviewed by the OCIO, at a minimum, on a quarterly basis. The OCIO should utilize the quarterly review of POA&Ms to assess the timeliness of corrective actions and the appropriateness of resources applied to the corrective actions. The periodic reviews should entail:

- Descriptions of the identified security weaknesses, including severity
- Methods used to identify the security weaknesses
- Identification of the GPO function responsible for resolving the weaknesses
- Estimated resources needed to mitigate the weaknesses
- Planned milestones and completion dates
- Status of corrective actions

7) POA&Ms should continue to be reviewed periodically by the GPO OIG to help ensure independent verification and validation of identified weaknesses and planned corrective actions.

8) The POA&M process should be coordinated with GPO's IT capital planning efforts to help ensure that security costs are linked to actual system security performance.

Finding 2008-FISMA-04: Contingency Planning

Condition

System contingency plans have not been completed and tested for several key GPO systems, notably GPO Web Hosting, GPO Access, PPPS, and the Secure Card Personalization System (SECAPS) for the Trusted Traveler Program (TTP). Similar weaknesses were identified in the fiscal year 2007 FISMA evaluation report, and GPO has taken some corrective actions. For example, a Business Impact Analysis (BIA) was completed during the first quarter of fiscal year 2008, and the results are being used to finalize contingency planning efforts for GPO's general support system. System-specific contingency plans will then be developed to complement the general support system contingency plan.

Criteria

FISMA requires:

> "Each agency shall develop, document, and implement an agency-wide information security program, approved by the Director under section 3543(a)(5), to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source, that includes plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency."

GPO Publication 825.33, "Information Technology Security Program Statement of Policy", requires:

> "The GPO will safeguard its IT systems through the implementation of the GPO IT Security Program, which will accomplish the following: define, document, and manage the contingency planning process, including training and testing, to provide IT systems with adequate continuity of operations upon disruption of normal operations.
>
> The CIO is responsible for developing and maintaining an agency-wide IT Security Program, including providing for the continuity of operations in the event of system disruption.
>
> Contingency plan means a plan for emergency response, back-up operations, and post-disaster recovery for IT systems and installations in the event normal operations are interrupted. The contingency plan should ensure minimal impact

> upon data processing operations in the event the IT system or facility is damaged or destroyed."

NIST SP 800-34, "Contingency Planning Guide for Information Technology Systems", states:

> "IT and automated information systems are vital elements in most business processes. Because these IT resources are so essential to an organization's success, it is critical that the services provided by these systems are able to operate effectively without excessive interruption. Contingency planning supports this requirement by establishing thorough plans and procedures and technical measures that can enable a system to be recovered quickly and effectively following a service disruption or disaster."

Cause

GPO recognizes the need to complete contingency plans for key systems, but competing priorities have limited the Agency's abilities to complete all necessary contingency plans.

Effect

Without effective contingency planning, which includes periodic testing of the plan's accuracy and reliability, GPO may be unable to access critical information and resources and perform mission critical business functions during an extended outage and/or disaster. Further, key parties and responsible individuals may not fully understand their roles and responsibilities during the execution of the plan. As a result, GPO may be unable to resume operations in an efficient and effective manner and meet its customers' demands for products and services.

Recommendations

9) GPO should continue the development of its business resumption and contingency planning efforts in accordance with NIST SP 800-34, "Contingency Planning Guide for Information Technology Systems" to enable appropriate contingency support to mission critical systems and business functions.

10) Upon the completion of the contingency plans, GPO should provide training to appropriate personnel, perform periodic testing of the plans, and update the plans based on the results of the testing. Test plans should address system recovery from backup media on an alternate platform, coordination among recovery teams, internal and external connectivity, performance of systems when using alternate equipment, restoration of normal operations, and notification procedures.

Finding 2008-FISMA-05: Incident Reporting

Condition

The GPO "Computer Security Incident Response Team (CSIRT) Framework and Procedures" do not address all of the elements outlined in NIST SP 800-61, "Computer Security Incident Handling Guide." Specifically, the following exceptions were noted:

- Guidance was not provided in the CSIRT Framework and Procedures regarding the prioritization of incidents.

- Timelines for reporting security incidents to the Department of Homeland Security (DHS) US-CERT are not documented.

Similar weaknesses were identified in the fiscal year 2007 FISMA evaluation report.

Additionally, GPO has not developed specific procedures for reporting incidents of Personally Identifiable Information (PII) exposures, as required by OMB Memo M-07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information."

Criteria

FISMA requires:

> "Each agency shall develop, document, and implement an agency-wide information security program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source, that includes procedures for detecting, reporting, and responding to security incidents, consistent with standards and guidelines issued pursuant to section 3546(b), including:
>
> - Mitigating risks associated with such incidents before substantial damage is done;
>
> - Notifying and consulting with the Federal information security incident center referred to in section 3546; and
>
> - Notifying and consulting with, as appropriate law enforcement agencies and relevant Offices of Inspector General, an office designated by the President for any incident involving a national security system; and, any

other agency or office, in accordance with law or as directed by the President."

DHS US-CERT Federal Incident Reporting Guidelines require:

"In order to clearly communicate incidents and events (any observable occurrence in a network or system) throughout the Federal Government and supported organizations, it is necessary for the government incident response teams to adopt a common set of terms and relationships between those terms. All elements of the Federal government should use a common taxonomy. Below please find a high level set of concepts and descriptions to enable improved communications among and between agencies. The taxonomy below does not replace discipline (technical, operational, intelligence) that needs to occur to defend federal agency computers/networks, but provides a common platform to execute the US-CERT mission. US-CERT and the federal civilian agencies are to utilize the following incident and event categories and reporting timeframe criteria as the Federal agency reporting taxonomy."

Federal Agency Incident Categories

Category	Name	Description	Reporting Timeframe
CAT 0	Exercise/Network Defense Testing	This category is used during state, federal, national, international exercises and approved activity testing of internal/external network defenses or responses.	Not Applicable; this category is for each agency's internal use during exercises.
CAT 1	Unauthorized Access	In this category, an individual gains logical or physical access without permission to a federal agency network, system, application, data, or other resource.	Within one (1) hour of discovery/ detection.
CAT 2	Denial of	An attack that	Within two

Category	Name	Description	Reporting Timeframe
	Service (DoS)	successfully prevents or impairs the normal authorized functionality of networks, systems or applications by exhausting resources. This activity includes being the victim or participating in the DoS.	(2) hours of discovery/ detection if the successful attack is still ongoing and the agency is unable to successfully mitigate activity.
CAT 3	Malicious Code	Successful installation of malicious software (e.g., virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system or application. Agencies are NOT required to report malicious logic that has been successfully quarantined by antivirus (AV) software.	Daily Note: Within one (1) hour of discovery/ detection if widespread across agency.
CAT 4	Improper Usage	A person violates acceptable computing use policies.	Weekly
CAT 5	Scans/Probes /Attempted	This category includes any	Monthly

Category	Name	Description	Reporting Timeframe
	Access	activity that seeks to access or identify a federal agency computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or denial of service.	Note: If system is classified, report within one (1) hour of discovery.
CAT 6	Investigation	Unconfirmed incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review.	Not Applicable; this category is for each agency's use to categorize a potential incident that is currently being investigated.

OMB Memorandum M-07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information", guides:

> "Each agency should develop a breach notification policy and plan comprising the elements discussed [in the memorandum]. In implementing the policy and plan, the Agency Head will make final decisions regarding breach notifications."
>
> "Agencies must report all incidents involving PII to US-CERT. This reporting requirement does not distinguish between potential and confirmed breaches. The

US-CERT concept of operations for reporting Category 1 incidents is modified as follows: Category 1: Unauthorized Access or Any Incident Involving Personally Identifiable Information. In this category agencies must report when: 1) an individual gains logical or physical access without permission to a federal agency network, system, application, data, or other resource; or 2) there is a suspected or confirmed breach of personally identifiable information regardless of the manner in which it might have occurred. Reporting to US-CERT is required within one hour of discovery/detection."

Cause

GPO recognizes the need to have more complete incident and breach of PII reporting processes and guidelines, but competing priorities have limited the Agency's abilities to do so.

Effect

An effective incident response capability is necessary to quickly detect security incidents, minimize loss and destruction, mitigate the weaknesses, and restore computing services. An inadequate incident response capability could delay the detection, mitigation, and restoration of IT and business processing in the event of an attack.

Recommendation

11) GPO should ensure that a complete and comprehensive process is in place for identifying, reporting, and resolving computer security incidents. As part of this process, the incident response procedures should:

- Include clear and comprehensive guidance for the identification, prioritization, and notification of security incidents internally and externally and to the US-CERT. This guidance should also include criteria for the identification of security incidents, including internal and external network-based attacks on GPO's IT infrastructure, as well as physical theft or loss of IT assets.

- Specifically develop a policy and procedures for responding to security incidents involving the breach of PII, whether in electronic or paper format.

Finding 2008-FISMA-06: Privacy and PII

Condition

GPO has not fully implemented controls necessary to identify, protect, and limit the use of PII. Specifically:

- Privacy Impact Assessments (PIAs) have not been performed for GPO Access, GPO Web Hosting, PPPS, and SECAPS.

- GPO has not developed and implemented a plan to eliminate the unnecessary use of PII such as Social Security Numbers (SSNs).

- Users with authorized access to PII are not required to reconfirm the acceptance of their responsibilities in writing on an annual basis.

- GPO partially deployed a full disk encryption process during fiscal year 2008, which can effectively facilitate the protection of PII, but not all Agency mobile devices have been equipped yet with the encryption software.

Similar weaknesses were identified in the fiscal year 2007 FISMA evaluation report.

Criteria

The Privacy Act of 1974 (Privacy Act) requires each agency to:

- "Establish Rules of Conduct. Agencies are required to establish rules of conduct for persons involved in the design, development, operation, or maintenance of any system of records, or in maintaining any record, and instruct each such person with respect to such rules and the requirements of the Privacy Act, including any other rules and procedures adopted pursuant to the Privacy Act and the penalties for noncompliance.

- Establish Safeguards. Agencies are also required to establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience or unfairness to any individual on whom information is maintained.

- Maintain accurate, relevant, timely and complete information. The Privacy Act also requires personally identifiable information within a system of records to be maintained in a manner that is accurate, relevant, timely, and complete

> including through the use of notices to the public. It is important for agencies to fulfill their responsibilities with respect to identifying systems of records and developing and publishing notices as required by the Privacy Act and OMB's implementing policies. By collecting only the information necessary and managing it properly, agencies can often reduce the volume of information they possess, the risk to the information, and the burden of safeguarding it."

Note that similar to FISMA, as a Legislative branch agency GPO is not required by law to adhere to Privacy Act requirements, but the Agency has recognized the Privacy Act as a best practice so we include it as criteria for this evaluation.

FISMA requires each agency to:

> "Develop, document, and implement an agencywide information security program…to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source…"

OMB Memorandum M-07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information", guides that agencies should:

> "Encrypt, using only NIST certified cryptographic modules, all data on mobile computers/devices carrying agency data unless the data is determined not to be sensitive, in writing, by your Deputy Secretary or a senior-level individual he/she may designate in writing."

Cause

GPO has not designated a responsible official (e.g., Chief Privacy Officer) for managing and monitoring the Agency's privacy compliance efforts. As a result, privacy requirements have not been adequately identified and subsequently communicated to other responsible program officials (e.g. OCIO). Additionally, competing priorities have prevented the completion of PIAs for key GPO systems (GPOAccess, GPO Web Hosting, PPPS) and the full deployment of planned disk encryption for mobile devices.

Effect

Without the proper identification, protection, and limitation of the use of PII, GPO systems and devices containing PII may be susceptible to unidentified threats and security weaknesses. Additionally, the use of PII may not be adequately restricted, thereby leading to the improper dissemination of sensitive information. As a result, unauthorized persons may gain access to valuable resources and sensitive information.

Recommendations

12) GPO should designate a responsible official (e.g., Chief Privacy Officer) for managing and monitoring the Agency's privacy compliance efforts. The designated official should participate in GPO's information privacy compliance activities, evaluate the ramifications for privacy of legislative, regulatory, and other policy proposals, and participate in assessing the impact of technology on PII.

13) To comply with requirements of OMB Memorandum M-07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information", we recommend that GPO develop a policy concerning the responsibilities of individuals authorized to access PII and implement: 1) a plan to eliminate the unnecessary use of PII, including the identification of suitable alternatives, and 2) a policy requiring users with authorized access to PII to reconfirm in writing the acceptance of their responsibilities to protect PII from misuse and exposure on an annual basis.

14) GPO should continue with plans to encrypt data on all portable devices.

15) GPO should complete PIAs for each of its major systems (e.g. GPO Access, GPO Web Hosting, PPPS, and the SECAPS).

Finding 2008-FISMA-07: System Security Plans

Condition

System security plans address the controls necessary to adequately mitigate identified security risks to an acceptable level, and are key components of the system C&A process. However, system security plans have not been developed for all of GPO's major systems in accordance with NIST SP 800-18, "Guide for Developing Security Plans for Federal Information Systems." Specifically, system security plans have not been completed for GPO Web Hosting and GPO Access. Similar weaknesses were identified in the fiscal year 2007 FISMA evaluation report.

Criteria

FISMA requires:

> "Each agency shall develop, document, and implement an agency-wide information security program, approved by the Director, to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source, that includes subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate."

NIST SP 800-18, "Guide for Developing Security Plans for Information Technology Systems", guides:

> "The purpose of the system security plan is to provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements. The system security plan also delineates responsibilities and expected behavior of all individuals who access the system. The system security plan should be viewed as documentation of the structured process of planning adequate, cost-effective security protection for a system.
>
> All information systems must be covered by a system security plan and labeled as a major application1 or general support system. Specific system security plans for minor applications are not required because the security controls for those applications are typically provided by the general support system or major application in which they operate."

NIST SP 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems", guides:

> "The assessment of risk and the development of system security plans are two important activities in an agency's information security program that directly support security accreditation and are required by FISMA and OMB Circular A-130, Appendix III. Risk assessments influence the development of the security controls for information systems and generate much of the information needed for the associated system security plans."

Cause

GPO recognizes the need to have documented system security plans for all major systems, but competing priorities have limited the Agency's abilities to do so.

Effect

Without complete and comprehensive system security plans that document planning activities undertaken by GPO to protect IT resources, the risk is elevated for: 1) not effectively communicating the importance of system security to users, and 2) not providing a basis by which management can ensure the effectiveness of security measures. System security plans allow GPO to have complete and comprehensive plans that provide an overview of the security requirements and describes the controls in place or planned for meeting those requirements.

Recommendation

16) GPO should ensure that security plans are completed for each major system. The security plans should completely, accurately, and comprehensively address all required elements of NIST SP 800-18, "Guide for Developing Security Plans for Federal Information Systems."

Finding 2008-FISMA-08: Risk Assessments

Condition

Prior to the development of the system security plan, a risk assessment must first be performed for each major application or general support system to determine the risks posed to each respective system. Once finalized, the output of the risk assessment should be used to determine the appropriate level of controls needed to adequately protect each information system from the threats identified. These controls should be adequately and completely documented in the system security plan. Despite the importance of security risk assessments, GPO has not performed risk assessments for GPO Web Hosting, GPO Access, PPPS, and the SECAPS in accordance with NIST SP 800-30, "Risk Management Guide for Information Technology." A similar weakness was identified in the fiscal year 2007 FISMA evaluation report.

Criteria

FISMA requires:

> "The head of each agency shall ensure that senior agency officials provide information security for the information and information systems that support the operations and assets under their control, including through assessing the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of such information or information systems.
>
> Each agency shall develop, document, and implement an agency-wide information security program, approved by the Director, to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source, that includes: periodic assessments of the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency and policies and procedures that are based on the risk assessments."

NIST SP 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems", guides:

> "The assessment of risk and the development of system security plans are two important activities in an agency's information security program that directly support security accreditation and are required by FISMA and OMB Circular A-130, Appendix III. Risk assessments influence the development of the security

controls for information systems and generate much of the information needed for the associated system security plans."

Cause

GPO recognizes the need to have documented risk assessments, but competing priorities have limited the Agency's abilities to do so.

Effect

Without the performance of a comprehensive documented risk assessment for each key system, GPO may not successfully identify the security risks posed by the operation of the system. As a result, GPO may not adequately monitor and mitigate risks to a level deemed acceptable by Agency management.

Recommendations

17) GPO should complete risk assessments for its major applications and systems, including GPO Web Hosting, GPO Access, Passport Production, and SECAPS, in accordance with the guidance outlined in NIST SP 800-30, "Risk Management Guide for Information Technology Systems." Further, system owners should accept any residual risk associated with the assessments. The acceptance of residual risk should be reviewed and formally documented by the OCIO.

18) Upon the completion of the risk assessments, GPO should determine the appropriate levels of controls that are needed to adequately protect each information system from the threats identified. The controls should be adequately and completely documented in the related system security plans per the guidance outlined in the NIST SP 800-18, "Guide for Developing Security Plans for Federal Information Systems."

Finding 2008-FISMA-09: C&A Process

Condition

GPO Web Hosting, GPO Access, and PPPS did not receive C&As prior to implementation into the production environment. Interim Authorities to Operate (IATOs) were granted for the SECAPS and Secure Production Facility (SPF) rather than the full C&A. Although an IATO does grant a limited authority to operate, it does not constitute the FISMA-required full C&A.

Criteria

GPO Publication 825.33, "Information Technology Security Program Statement of Policy", requires:

> "Authorized Processing – C&A. Certification is the evaluation of IT system(s) security controls to ensure they are implemented and to determine the residual risk. Accreditation is the acceptance by the Designated Approving Authority (DAA) of the residual risk by senior management, based on threats to the system and the implemented security controls. (The DAA may grant interim authority to operate on a case-by-case basis.) Systems will undergo C&A before they process any data. Additionally, systems will be re-accredited at least every 3 years, or when a significant change is made to the configuration of the system."

NIST SP 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems" guides:

> "The successful completion of the security certification and accreditation process provides agency officials with the necessary confidence that the information system has adequate security controls, that any vulnerabilities in the system have been considered in the risk-based decision to authorize processing, and that appropriate plans and funds have been identified to correct any deficiencies in the information system."

Cause

GPO recognizes the need to have complete C&A packages for Agency systems, but competing priorities have limited the Agency's abilities to do so.

Effect

Without full C&As for GPO major applications and systems, the Agency may not be sufficiently identifying and mitigating the security risks posed by the introduction of new

or revised applications and systems into the production environment. As a result, applications and systems may operate in the production environment without appropriate controls or management oversight.

Recommendations

19) GPO should continue its efforts to complete the C&A of its major applications and systems in accordance with NIST SP 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems." These efforts should include the development and maintenance of documentation used in the certification process and the security accreditation decision (e.g. risk assessments, system security plans, and contingency plans).

20) GPO should maintain a schedule to track C&A life cycle activities of each major application and general support system. This schedule should include:

- The stage of the C&A process for each system (i.e., IATO or full authority to operate) and the expected date of authorization.

- The completion date or expected completion date of each component of the certification and accreditation process, including system security plans, contingency plans, and risk assessments.

- If authorized, the schedule should also include the projected date of re-certification.

The system owner's name and contact information should be identified for each system.

Finding 2008-FISMA-10: System Security Configuration Management and Patch Management Processes

Condition

GPO has not fully implemented controls to ensure the security configuration of systems, notably the Microsoft Windows operating system, Microsoft Internet Information Server (IIS), and Oracle database management system. This condition has been reported in prior GPO financial statement audits and GPO Office of Inspector General (OIG) reports, including the 2007 FISMA evaluation report. In response to prior year findings, GPO began implementing the Configuresoft Security Update Manager (SUM) software to more effectively monitor the security configurations for key systems and the software patch management process. However, the tool has not been fully implemented. As a complement to the use of the Configuresoft SUM, GPO also relies on periodic vulnerability scans to validate the security configuration for key systems.

Criteria

FISMA requires:

> "Each agency to ensure compliance with minimally acceptable system configuration requirements."

Cause

Competing resources have limited GPO's ability to fully implement the Configuresoft SUM.

Effect

Although use of a vulnerability scanning process may identify non compliance with system security configurations, the process does not provide a complete assessment of the security configurations. For example, system and device configurations, such as audit settings, file permissions, account permissions, and administrator/root usage may not be fully assessed for compliance with GPO's security configuration baseline. Further, the vulnerability assessment process does not provide a real time assessment of security configurations, which the Configuresoft SUM tool provides.

Recommendations

21) GPO should continue with plans to implement the Configuresoft SUM tool to more effectively manage real time system security configurations.

Appendix A. Management's Response

MEMORANDUM

DATE: October 16, 2009

REPLY TO ATTN OF: Chief Information Officer

SUBJECT: IT&S Response: Draft OIG Assessment Report on GPO FISMA Compliance

TO: Office of the Inspector General

Introduction

The Office of the Inspector General (OIG) issued a Draft Report on August 7, 2009, concerning an assessment of the GPO compliance with the Federal Information Security Management Act (FISMA). The date of the draft report is July 15, 2009 and it was transmitted to IT&S via letter from the OIG dated August 7, 2009.

This document is the GPO Information Technology and Systems (IT&S) response to the OIG recommendations contained in that Assessment Report.

OIG Recommendations and IT&S Response

The results of the Draft FISMA Assessment Report indicated, as was expected by GPO management, several areas in which GPO made progress and some areas in which opportunities for improvement exist. IT&S completed the Certification and Accreditation (C&A) process for several new major applications and systems since the last OIG FISMA Assessment, including FDsys, GBIS, General Support System #1, and the Secure Card Personal System for Inaugural Credentials. The opportunities for improvement were expected in that GPO was not able to invest in the combination of additional tools, equipment and staff that would have been necessary to fully address the entire spectrum of FISMA controls and requirements. It should be noted that as a Legislative Branch organization FISMA does not directly apply to GPO, however since GPO serves all three (3) branches of federal government, GPO is interested in assessing its operations and IT systems against the FISMA standard used in the Executive Branch. The IT&S response to each of the OIG findings is shown below.

OIG Recommendation #1:

GPO's should enhance the existing system inventory to ensure it contains all major Agency systems and supporting interfaces and peripheral equipment.

IT&S Response:

IT&S agrees that enhancements to the system inventory would be beneficial to the control environment. The BDNA software utility has been operationally enhanced which should provide for a comprehensive capability for listing peripheral equipment and devices. GPO Enterprise Architecture Repository (System Architect software) contains existing inventory of all major Agency systems with description of the major interfaces. All major GPO systems are also mapped in this Repository to technologies they utilize. In addition, the GPO Architecture Review

Board (ARB) has been established and is operational, which provides for an enhanced visibility and control on any new agency applications and systems. The capabilities afforded now by the BDNA tool, EA Repository and the ARB process enable IT&S to address this.

Thus, we believe this recommendation has been addressed and can be closed.

OIG Recommendation #2:

The results of the periodic network and system scanning activities should be used to assist in reconciling and validating the inventory listings.

IT&S Response:

IT&S agrees that when the inventory process is mature, this type of reconcilement will be included. The first priority is to provide complete system inventory so that this scanning reconcilement activity will be meaningful and not wasted effort. There will also be training and procedure development required in order to address this recommendation. Therefore, it is expected that this type of reconcilement process using network scanning could be made operational by December 31, 2009.

OIG Recommendation #3:

To support Recommendation #1, detailed procedures should be developed to describe the process the business units should use to include systems in the Agency inventory.

IT&S Response:

The process by which agency business areas and any GPO unit requests a new system (such as application, server or device) be added to the Agency inventory has been discussed extensively within IT&S and follows the GPO EA, ARB and SDLC process. The ARB has representatives from the Business Units and facilitates the addition or modification of the agency inventory. Documenting this procedure is expected to be complete by October 31, 2009.

OIG Recommendation #4:

GPO should take action to fully implement the FISMA and Agency security requirements to perform periodic security reviews for key systems. The reviews should be conducted in accordance with NIST SP 800-53A, "Guide for Assessing Security Controls in Federal Information Systems". Specifically, the security reviews should document scope of the reviews, the procedures to be performed, and the results of the reviews. Further, the system certification and accreditation (C&A) packages (e.g., risk assessments, security plans) should be updated as needed based on the reviews.

IT&S Response:

IT&S agrees that periodic security reviews for key systems are a valuable component of the agency's security program. Such reviews take resources, in terms of personnel time, including those of business units. Presently, periodic vulnerability assessment scans are conducted by IT&S, which consumes IT Security group resources available for such periodic reviews. To expand the scope of periodic security reviews to include additional security assessment and testing will require additional resources. An assessment of the additional resource requirements associated with this OIG recommendation will be prepared by IT&S for review by GPO management. IT&S expects to have the resource assessment completed by October 31, 2009 so that management can start its deliberations on that date.

Appendix A

OIG Recommendation #5:

GPO's POA&M process should include procedures for tracking and monitoring the status of system-specific weaknesses and the development of executive-level summaries for the POA&Ms.

IT&S Response:

IT&S agrees with this recommendation and has made significant progress on this topic. The IT Security group held a set of POA&M workshops during July-August 2009 with the CIO, IT Directors and other agency parties for the identified security weaknesses for all GPO systems. The weaknesses were compiled from all known OIG and other audit recommendations, from open items in IT&S conducted Certification and Accreditation (C&A) assessments, and from significant IT&S vulnerability assessment open items that remained open after more than one (1) quarter. A final meeting with the CIO and IT&S Directors to review the Planned Actions and Milestone Dates is being scheduled for September 2009.

OIG Recommendation #6:

POA&Ms should be periodically reviewed by the OCIO, at a minimum, on a quarterly basis. The OCIO should utilize the quarterly review of POA&Ms to assess the timeliness of corrective actions and the appropriateness of resources applied to the corrective actions.

The periodic reviews should entail:

Descriptions of the identified security weaknesses, including severity
Methods used to identify the security weaknesses
Identification of the GPO function responsible for resolving the weaknesses
Estimated resources needed to mitigate the weaknesses
Planned milestones and completion dates
Status of corrective actions

IT&S Response:

IT&S completed a set of POA&M workshops, which included the CIO and IT Directors, on August 24, 2009 with responsible IT and other agency parties for the identified security weaknesses for all GPO systems. The weaknesses were compiled from: 1) all known OIG and other audit recommendations; 2) from open items in IT&S conducted Certification and Accreditation (C&A) assessments; and 3) from significant IT&S vulnerability assessment open items that remained open after more than one (1) quarter. A final meeting with the CIO and IT&S Directors to review the Planned Actions and Milestone Dates is being scheduled for September 2009. This will be the first of a planned quarterly review cycle for the POA&M templates for GPO systems.

OIG Recommendation #7:

POA&Ms should continue to be reviewed periodically by the GPO OIG to help ensure independent verification and validation of identified weaknesses and planned corrective actions.

IT&S Response:

This is not a recommendation for IT&S to take any action on. Therefore, there is no IT&S response required. IT&S does not have any concerns or issues with the recommendation.

OIG Recommendation #8:

The POA&M process should be coordinated with GPO's IT capital planning efforts to help ensure that security costs are linked to actual system security performance.

IT&S Response:

IT&S has involved all IT Directors, including the CIO and Director of Enterprise Architecture (EA), in the POA&M process. This provides direct linkage into the EA process and IT capital planning process at GPO. In addition, GPO has enhanced the EA process during FY2009 providing better documentation and linkages for IT items to the agency capital planning and investment review process. Since the CIO and IT Security are explicitly included in the agency's EA process, the POA&M items are therefore included and linked into the agency's IT capital planning efforts.

IT&S therefore believes this item is resolved and can be closed.

OIG Recommendation #9:

GPO should continue the development of its business resumption and contingency planning efforts in accordance with NIST SP 800-34, "Contingency Planning Guide for Information Technology Systems" to enable appropriate contingency support to mission critical systems and business functions.

IT&S Response:

This recommendation goes beyond IT&S and includes all the agency business functions, whose business COOP plans affect the IT&S Contingency Plan. The Contingency Plan for IT&S systems continues to be enhanced and made more comprehensive. The agency's overall identification of mission critical systems and business functions (along with the sequencing for restoration) has also been enhanced during FY2009, however it also requires further efforts, which when complete will assist IT&S in identifying the complete set of IT systems and contingency plan procedures necessary to support those business needs.

OIG Recommendation #10:

Upon the completion of contingency plans for each of the GPO's major systems, the Agency should provide training to appropriate personnel, perform periodic testing of the plans, and update the plans based on the results of the testing. Test plans should address system recovery from backup media on an alternate platform, coordination among recovery teams, internal and external connectivity, performance of systems when using alternate equipment, restoration of normal operations, and notification procedures.

IT&S Response:

This recommendation goes beyond IT&S and includes all agency business functions. GPO conducted a major Congressional support Contingency test on August 29-30, 2009. GPO also successfully conducted its annual PKI Contingency Test in June 2009. A plan that would address the procedures for all the major applications is a major effort, which will require multiple years to complete.

OIG Recommendation #11:

GPO should develop a complete and comprehensive process for identifying, reporting, and resolving computer security incidents, as well as developing a PII breach notification policy covering both electronic and paper breaches of PII.

IT&S Response:

GPO's Computer Security Incident Response Team (CSIRT) Procedures document provides a complete set of procedures for identifying, reporting and resolving computer security incidents. PII breach notification policy is an area that requires coordination among several areas of GPO, including the Office of General Counsel (OGC), CMO, CHCO, CIO and others. The Office of the General Counsel (OGC) has produced an initial draft of a framework for PII, and coordinated it with IT&S, that addresses this recommendation. IT&S will work with OGC and other GPO organizational elements on the GPO approach to PII breach notification.

OIG Recommendation #12:

GPO should designate a responsible official (e.g., Chief Privacy Officer) for managing and monitoring the Agency's privacy compliance efforts. The designated official should participate in GPO's information privacy compliance activities, evaluate the ramifications for privacy of legislative, regulatory, and other policy proposals, and participate in assessing the impact of technology on PII.

IT&S Response:

The Office of the General Counsel (OGC) has produced an initial draft of a framework for PII, and coordinated it with IT&S, that addresses this recommendation. IT&S will work with OGC and other GPO organizational elements on the GPO approach to PII protection. This recommendation goes beyond IT&S and is agency wide, involving the OGC, Human Capital Office, and business units among others.

OIG Recommendation #13:

To comply with requirements of OMB Memorandum M-07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information", we recommend that GPO develop a policy concerning the responsibilities of individuals authorized to access PII and implement: 1) a plan to eliminate the unnecessary use of PII, including the identification of suitable alternatives, and 2) a policy requiring users with authorized access to PII to reconfirm in writing the acceptance of their responsibilities to protect PII from misuse and exposure on an annual basis.

IT&S Response:

The Office of the General Counsel (OGC) has produced an initial draft of a framework for PII, and coordinated it with IT&S, that addresses this recommendation. IT&S will work with OGC and other GPO organizational elements on the GPO approach to PII protection. This recommendation goes beyond IT&S and is agency wide, involving the OGC, Human Capital Office, and business units among others.

OIG Recommendation #14:

GPO should continue with plans to encrypt data on all portable devices.

IT&S Response:

IT&S has been actively deploying software (Pointsec) to comply with this recommendation to agency mobile PC's (laptops) during FY2009. This takes two (2) forms: 1) deployment to new laptops that are provisioned; and 2) deployment to legacy laptops. Process #1 for integration of Pointsec into the standard laptop deployment process for new laptops is completed as of February 2009. Process #2 for deployment to legacy (previously deployed) laptops is a resource intensive task. It is expected that the deployment of Pointsec to all legacy GPO laptop computers can be completed by September 30, 2010.

OIG Recommendation #15:

GPO should complete a Privacy Impact Assessment (PIA) for key systems.

IT&S Response:

IT&S agrees that Privacy Impact Assessments should be completed for key systems. Many key systems (PKI, Secure Card Personalization System, GBIS, and FDsys) were completed during FY2009. This is a resource issue in terms of accomplishing this recommendation for all remaining and new key systems, along with all the other FISMA recommendations and other IT Security program operational requirements. IT&S will develop a resource impact assessment that estimates the required investments by October 1, 2009.

OIG Recommendation #16:

GPO should ensure that security plans are completed for each major system. The security plans should completely, accurately, and comprehensively address all required elements of NIST SP 800-18, "Guide for Developing Security Plans for Federal Information Systems."

IT&S Response:

IT&S agrees with the recommendation. Many major systems (GBIS, FDsys, PKI, Passport, Secure Card Personalization System, and others) already have SSP's. This is a resource issue in terms of accomplishing this recommendation for all remaining and new key systems, along with all the other FISMA recommendations and other IT Security program operational requirements. IT&S will develop a resource impact assessment which estimates the required investments for this by October 1, 2009.

OIG Recommendation #17:

GPO should complete risk assessments for its major applications and systems in accordance with the guidance outlined in NIST SP 800-30, "Risk Management Guide for Information Technology Systems." Further, system owners should accept any residual risk associated with the assessments. The acceptance of residual risk should be reviewed and formally documented by the OCIO.

IT&S Response:

IT&S agrees with the recommendation. Many major systems (GBIS, FDsys, PKI, Passport, Secure Card Personalization System, and others) already have completed Risk Assessments. This is a resource issue in terms of accomplishing this recommendation for all remaining and new

key systems, along with all the other FISMA recommendations and other IT Security program operational requirements. IT&S will develop a resource impact assessment which estimates the required investments by October 1, 2009.

OIG Recommendation #18:

Upon the completion of the risk assessments, GPO should determine the appropriate levels of controls that are needed to adequately protect each information system from the threats identified. The controls should be adequately and completely documented in the related system security plans per the guidance outlined in the NIST SP 800-18, "Guide for Developing Security Plans for Federal Information Systems."

IT&S Response:

IT&S agrees with the recommendation however this appears to be closely related to Recommendation #16 and may be a duplicate. All SSP's contain what GPO considers to be the required security controls for the system. IT&S and GPO always include all the defined security controls that apply to a system in the SSP. Thus, while IT&S acknowledges that there are certain applications for which SSP's remain to be created for, we believe the SSP's already comply with this recommendation.

OIG Recommendation #19:

GPO should continue its efforts to complete the C&A of its major applications and systems in accordance with NIST SP 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems." These efforts should include the development and maintenance of documentation used in the certification process and the security accreditation decision (e.g. risk assessments, system security plans, and contingency plans).

IT&S Response:

IT&S agrees with the recommendation. Many major systems (GBIS, FDsys, PKI, Passport SPF, Secure Card Personalization System, and others) already have completed Certification and Accreditation. This is a resource issue in terms of accomplishing this recommendation for all remaining and new key systems, along with all the other FISMA recommendations and other IT Security program operational requirements. IT&S will develop a resource impact assessment (which will show estimated investments required to complete this) by October 1, 2009.

OIG Recommendation #20:

GPO should maintain a schedule to track C&A life cycle activities of each major application and general support system. This schedule should include:

- The stage of the C&A process for each system (i.e., IATO or full authority to operate) and the expected date of authorization.
- The completion date or expected completion date of each component of the certification and accreditation process, including system security plans, contingency plans, and risk assessments.
- If authorized, the schedule should also include the projected date of re-certification.

The system owner's name and contact information should be identified for each system.

IT&S Response:

IT&S agrees with this recommendation. Such a schedule will be developed for the known major applications and General Support System by September 30, 2009.

OIG Recommendation #21:

GPO should continue with plans to implement the Configuresoft SUM tool to more effectively manage real time system security configurations and the patch management process.

IT&S Response:

The Configuresoft tool is already deployed for server system patch management. Plans are to extend its use to desktop systems at GPO. IT&S will evaluate the resource and operational implications to using Configuresoft to perform real-time monitoring and management of server security configurations. That would have resource implications in terms of investment in additional automation and/or additional manpower. IT&S will assess the additional resource impact of the real-time management aspect and coordinate the results with GPO management. This assessment is expected to be completed by December 1, 2009.

MICHAEL L. WASH

Appendix B. Status of Recommendations

Recommendation No.	Resolved	Unresolved	Open/ECD*	Closed
1	X		10-31-09	
2	X		12-31-09	
3	X		10-31-09	
4	X		TBD	
5	X		9-30-09	
6	X		9-30-09	
7	X		12-31-09	
8	X		10-31-09	
9	X		TBD	
10	X		TBD	
11	X		TBD	
12	X		TBD	
13	X		TBD	
14	X		9-30-10	
15	X		TBD	
16	X		TBD	
17	X		TBD	
18	X		TBD	
19	X		TBD	
20	X		9-30-09	
21	X		TBD	

*Estimated Completion Date

Appendix C. Report Distribution

Deputy Public Printer
Acting Chief of Staff
Acting General Counsel
Chief Information Officer
Chief Technology Officer
Chief Management Officer
Chief Information Security Officer