




U.S. GENERAL SERVICES ADMINISTRATION
Office of Inspector General

DEC 16 2015

MEMORANDUM FOR: DENISE TURNER ROTH
ADMINISTRATOR (A)

FROM: CAROL F. OCHOA 
INSPECTOR GENERAL (J)

SUBJECT: Transmittal of the Fiscal Year 2015 Independent
Evaluation of the U.S. General Services
Administration's Compliance with the Federal
Information Security Modernization Act of 2014

This memorandum transmits KPMG LLP's (KPMG) evaluation of GSA's compliance with the *Federal Information Security Modernization Act of 2014* (FISMA) for fiscal year 2015.

FISMA requires Inspectors General, or an independent external auditor as determined by the Inspector General of the agency, to perform an annual evaluation of their agency's security program and practices. GSA contracted with KPMG, an independent public accounting firm, to assess its information security program in accordance with FISMA. The contract required that the evaluation be performed in accordance with the Council of the Inspectors General on Integrity and Efficiency's (CIGIE) *Quality Standards for Inspection and Evaluation* and the Office of Management and Budget's (OMB) FISMA reporting guidance.

In connection with the contract, we reviewed KPMG's report and related documentation and inquired of its representatives. Our review, as differentiated from an audit in accordance with generally accepted government auditing standards, was not intended to enable us to express, and we do not express, opinions on GSA's security program or conclusions about the effectiveness of internal control or on whether GSA's security program complied with FISMA; or conclusions on compliance with laws and regulations. KPMG is responsible for the attached report dated November 4, 2015, and the conclusions expressed in the report. However, our review disclosed no instances where KPMG did not comply with CIGIE's *Quality Standards for Inspection and Evaluation* and OMB's FISMA reporting guidance.

A draft report was provided to the GSA Office of the Chief Information Officer for review and comment. The Office of the Chief Information Officer's response to the draft report is attached in its entirety.

The fiscal year 2016 FISMA independent auditors will follow up on the outstanding recommendations and evaluate the adequacy of corrective actions.

We appreciate the courtesies and cooperation extended to KPMG and our audit staff by GSA during the evaluation. If you have any questions, please contact Theodore R. Stehney, Assistant Inspector General for Auditing, at (202) 501-0374.

Attachments



KPMG LLP
1676 International Drive, Suite 1200
McLean, VA 22102

Carolyn Presley-Doss
Deputy Assistant Inspector General for Audit Policy and Oversight
General Services Administration
Office of the Inspector General
1800 F St., NW, Suite 5306
Washington, DC 20405

December 3, 2015

Dear Ms. Presley-Doss,

We have submitted the following Federal Information Security Modernization Act (FISMA) reports for the General Services (GSA) Office of the Inspector General (OIG):

- *Fiscal Year 2015 U.S. General Services Administration Federal Information Security Modernization Act Systems Evaluation Report;*
- *Fiscal Year 2015 Independent Evaluation of the U.S. General Services Administration's Compliance with the Federal Information Security Modernization Act of 2014; and*
- *The U.S. General Services Administration Response to DHS's Federal Information Security Modernization Act Questions for Inspectors General For FY 2015.*

These reports were provided to you in this format pursuant to your written request as set forth in our Contract GS-H-00-15-AA-0098, Requisition Number PR20142030001, dated November 4, 2015 and is subject in all respects to the terms and conditions of, including restrictions on disclosure of this deliverable to third parties.

Detailed within the FY 2015 FISMA Reports are recommendations to address specific GSA- and system-level deficiencies within GSA's information security program and practices. When developing plans of actions and milestones (POA&Ms) or corrective actions, management should assess whether these deficiencies are contained to their respective areas as described in this report or whether the recommendations should be considered for other systems, security control areas, or processes within GSA's information system security program.

Please let me know if you have any questions.

Kind regards,

A handwritten signature in black ink, appearing to read 'James DeVaul', written in a cursive style.

James DeVaul
Partner, Federal Advisory Services

Fiscal Year 2015 Independent Evaluation of the U.S. General Services Administration's Compliance with the Federal Information Security Modernization Act of 2014

November 4, 2015



KPMG LLP
1676 International Drive, Suite 1200
McLean, VA 22102

**U.S. General Services Administration
Federal Information Security Modernization Act Fiscal Year 2015 Evaluation**

**Table of Contents
FISMA Evaluation Report**

| | |
|--|----|
| BACKGROUND | 3 |
| Federal Information Security Modernization Act | 3 |
| OVERALL EVALUATION RESULTS..... | 4 |
| FINDINGS..... | 5 |
| 1. Configuration Management..... | 5 |
| 2. Contingency Planning | 7 |
| 3. Risk Management..... | 9 |
| 4. Security Training..... | 12 |
| 5. Plan of Action and Milestones | 14 |
| MANAGEMENT RESPONSE TO THE REPORT | 15 |
| Appendices | |
| APPENDIX I – OBJECTIVE, SCOPE, AND METHODOLOGY..... | 17 |
| APPENDIX II – STATUS OF PRIOR YEAR FINDINGS..... | 20 |
| APPENDIX III – GLOSSARY..... | 25 |



KPMG LLP
1676 International Drive
McLean, VA 22102

Administrator and Inspector General
U.S. General Services Administration
1800 F Street, NW
Washington, DC 20405

**Re: Fiscal Year 2015 Independent Evaluation of the U.S. General Services Administration's
Compliance with the Federal Information Security Modernization Act of 2014**

This report presents the results of our independent evaluation of the U.S. General Services Administration's (GSA) information security program and practices. The Federal Information Security Modernization Act of 2014 (FISMA) requires federal agencies, including the GSA, to have an annual independent evaluation of their information security programs and practices and to report the results of the evaluations to the Office of Management and Budget (OMB). OMB has delegated its responsibility for the collection of annual FISMA responses to the Department of Homeland Security (DHS). FISMA requires that the agency Inspector General (IG) or an independent external auditor perform the independent evaluation as determined by the IG. The GSA contracted with KPMG LLP (KPMG) to conduct this independent evaluation.

We conducted our independent evaluation in accordance with the Council of the Inspectors General on Integrity and Efficiency's Quality Standards for Inspection and Evaluation.

The objective for this independent evaluation was to assess the effectiveness of the GSA's information security program and practices for the period October 1, 2014 to September 30, 2015 for its information systems, including the GSA's compliance with FISMA and related information security policies, procedures, standards, and guidelines. We based our work, in part, on a selection of GSA-wide security controls and a selection of system-specific security controls across five selected GSA information systems and five GSA contractor information systems. Additional details regarding the scope of our independent evaluation are included in Appendix I, *Objective, Scope & Methodology*.

Consistent with applicable FISMA requirements, OMB policy and guidelines, and the National Institute of Standards and Technology (NIST) standards and guidelines, the GSA's information security program and practices for its information systems have been established and are maintaining security programs for the ten FISMA program areas.¹ However, while the security program has been implemented across GSA, we identified the following five of ten FISMA program areas that had deficiencies:

1. Configuration management
2. Contingency planning
3. Risk management
4. Security training
5. Plan of actions and milestones

¹ The 10 FISMA program areas are continuous monitoring management, configuration management, identity and access management, incident response and reporting, risk management, security training, plan of action and milestones, remote access management, contingency planning, and contractor systems.



We have made 13 recommendations related to these control deficiencies that, if effectively addressed by management, should strengthen the respective information systems and the GSA's information security program. In a written response, the GSA Chief Information Officer (CIO) agreed with our findings and recommendations (see *Management Response*).

This independent evaluation did not constitute an engagement in accordance with *Government Auditing Standards*. KPMG did not render an opinion on the GSA's internal controls over financial reporting or over financial management systems as part of this evaluation. We caution that projecting the results of our evaluation to future periods or other information systems not included in our selection is subject to the risks that controls may become inadequate because of changes in technology or because compliance with controls may deteriorate.

Appendix I describes the FISMA evaluation's objective, scope, and methodology. Appendix II, *Status of Prior-Year Findings*, summarizes the GSA's progress in addressing prior-year recommendations. Appendix III contains a glossary of terms used in this report.

Sincerely,

KPMG LLP

November 4, 2015

BACKGROUND

Federal Information Security Modernization Act

Title III of the E-Government Act of 2002 (the Act), which was amended in 2014, commonly referred to as FISMA, focuses on improving oversight of federal information security programs and facilitating progress in correcting agency information security weaknesses. FISMA requires federal agencies to develop, document, and implement an agency-wide information security program that provides 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. The Act assigns specific responsibilities to agency heads and IGs in complying with requirements of FISMA. The Act is supported by the OMB, agency security policy, and risk-based standards and guidelines published by NIST related to information security practices.

Under FISMA, agency heads are responsible for providing information security protections commensurate with the risk and magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems. Agency heads are also responsible for complying with the requirements of FISMA and related OMB policies and NIST procedures, standards, and guidelines. FISMA directs federal agencies to report annually to the OMB Director, the Comptroller General of the United States, and selected congressional committees on the adequacy and effectiveness of agency information security policies, procedures, and practices. OMB has delegated some responsibility to the DHS in memorandum M-10-28, *Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security*, for the operational aspects of Federal cyber security, such as establishing government-wide incident response and operating the tool to collect FISMA metrics. In addition, FISMA requires agencies to have an annual independent evaluation performed of their information security programs and practices and to report the evaluation results to OMB. FISMA states that the independent evaluation is to be performed by the agency IG or an independent external auditor as determined by the IG.

OVERALL EVALUATION RESULTS

Consistent with applicable FISMA requirements, OMB policy, and NIST guidelines, the GSA has established an information security program and related practices for its systems. This program covers the 10 FISMA program areas outlined in the *FY 2015 Inspector General Federal Information Security Modernization Act Reporting Metrics* that were prepared by DHS's Office of Cybersecurity and Communications Federal Network Resilience. The program areas are:

- Continuous monitoring management;
- Configuration management;
- Identity and access management;
- Incident response and reporting;
- Risk management;
- Security training;
- Plan of action and milestones;
- Remote access management;
- Contingency planning; and
- Contractor systems.

However, while the security program has been implemented across the GSA, we identified deficiencies in five of ten FISMA program areas. We have made 13 recommendations related to these control deficiencies that, if effectively addressed by management, should strengthen the respective information systems and the GSA's information security program. The *Findings* section of this report presents the detailed findings and associated recommendations. In a written response to this report, the GSA CIO agreed with our findings and recommendations and provided corrective action plans (see *Management Response*). GSA's planned corrective actions are responsive to the intent of our recommendations.

Additionally, we evaluated the prior-year findings from the fiscal year (FY) 2014 FISMA Evaluation and noted that management had closed five of six findings. See Appendix II, *Status of Prior-Year Findings*, for additional details.

FINDINGS

1. Configuration Management

While performing our FISMA evaluation procedures we inspected GSA's configuration and vulnerability policy and procedural guides, conducted inquiries with individuals to walk through the process and determined that GSA has a configuration and vulnerability management program; however, we did identify the following exceptions:

- a. Evidence of review for WebInspect scans could not be provided for the two months selected for three of the five systems selected for testing.
- b. Evidence of critical and high information system's operating system and database vulnerabilities were not being remediated within 30 days for four of five of the systems selected for testing, but the vulnerabilities are tracked in GSA's scanning tool.
- c. Evidence of review of vulnerability scans by the TechOps Information System Security Officer (ISSO) could not be provided for four of five of the systems selected for testing.

The NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, RA-5, Vulnerability Scanning, page F-153, states

“The organization:

- c. Analyzes vulnerability scan reports and results from security control assessments;
- d. Remediates legitimate vulnerabilities [*Assignment: organization-defined response times*] in accordance with an organizational assessment of risk;”

GSA Order CIO P 2100.1I - GSA Information Technology (IT) Security Policy, October 20, 2014, page 40, states:

- a. “All critical and high vulnerabilities identified must be mitigated within 30 days and all moderate vulnerabilities mitigated within 90 days in accordance with IT Security Procedural Guide: Managing Enterprise Risk, OCIO-IT-06-30.”

GSA IT Risk Management Strategy, dated June 15, 2015, Version 1.0, page 16, states:

“6.1.5.2 Weekly/Monthly Scans: All GSA systems in the GSA enterprise architecture have scans performed on a weekly or monthly basis. Scan results are distributed to the responsible stakeholders (Authorizing Officials [AOs], Information System Security Managers [ISSMs], and Information System Security Officers [ISSOs]) and remediation efforts are performed accordingly.”

Management informed us that the review of vulnerability scan results is not documented, as it is inferred based on remediation change control documentation. Additionally, since there were no High or Critical vulnerabilities identified during the 2 months selected, there were no vulnerabilities tested that required remediation.

Tenable, a security vulnerability scanning management tool, is being used to scan for operating system baseline compliance, however it has been configured in accordance with GSA hardening guides to accurately reflect the configurations and the system setting to properly identify the deviations.

For certain operating system baseline compliance scans, GSA does remediate these items as they do not appear on the subsequent week scan, however, for the items that are not remediated within 30 days they still appear on the scans for GSA to remediate, and are tracked in Tenable as a plan of action and milestones (POA&M) entry is not required.

Lack of review documentation increases the risk that management may not timely identify instances where their employees are not reviewing results. If this occurs, the risk of vulnerabilities not being timely remediated increases.

The non-review, tracking and remediation of high and critical vulnerabilities increases the security risk to the confidentiality, integrity and availability of data.

We recommend that GSA perform the following actions:

1. Remediate high and critical vulnerabilities in-accordance within 30 days as required by GSA policy.
2. Maintain evidence that ISSOs or other designated individuals review of the operating system and database compliance, WebInspect and the vulnerability scan reports.

2. Contingency Planning

While performing our FISMA evaluation procedures we inspected GSA's contingency planning and backup policy and procedural guides, we conducted inquiries with individuals to walk through the process and determined that GSA has a contingency planning program and requires backups to be performed, however we did identify the following exceptions:

- a. Supply chain threats were not addressed for all five systems selected.
- b. There was no evidence that the Business Impact Analysis results were incorporated for three of the five systems selected for testing.
- c. The contingency plan was tested for only three of the five systems selected for testing.
- d. There was no evidence of having an alternate processing agreement for four of five systems selected for testing.
- e. Backups were not performed for two of the five systems selected for testing.

The NIST Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, CP-2, Contingency Plan, pg. F-78-80 states that:

“The organization:

- b. Distributes copies of the contingency plan to [*Assignment: organization-defined list of key contingency personnel (identified by name and/or by role) and organizational elements*];
- d. Reviews the contingency plan for the information system [*Assignment: organization-defined frequency*];
- e. Updates the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;
- f. Communicates contingency plan changes to [*Assignment: organization-defined list of key contingency personnel (identified by name and/or by role) and organizational elements*]; and
- g. Protects the contingency plan from unauthorized disclosure and modification.”

NIST SP 800-53, Rev.4, Control CP-9 Information System Backup, states that:

“The organization:

- b. Conducts backups of system-level information contained in the information system [*Assignment: organization-defined frequency consistent with recovery time and recovery point objectives*];
- c. Conducts backups of information system documentation including security-related documentation [*Assignment: organization-defined frequency consistent with recovery time and recovery point objectives*];

Control Enhancements:

- (1) The organization tests backup information [*Assignment: organization-defined frequency*] to verify media reliability and information integrity.”

The consolidation of all IT systems into the GSA IT division delayed the review of the Contingency Plans. This consolidation created the Information Systems Policy and Information Systems Engineering departments which are responsible for reviewing this plan. This plan is currently undergoing review and updates to be transitioned to NIST 800-53, Rev 4.

GSA did not provide a cause to why the contingency plan was not tested or why backups were not performed and they did not provide an alternate hosting agreement.

Not having a fully developed and documented Contingency Plan, testing the plan on a regular basis, having agreements in place for alternate processing sites, and performing backups increases the risk of a compromise of the confidentiality, integrity, and availability of the data residing on the information system in the event of a disaster.

We recommend that GSA perform the following actions:

1. Update the contingency plans to include the missing NIST required sections.
2. Schedule and perform an annual test of contingency plans to determine if it is effective and incorporate lessons learned from the test.
3. Work with all responsible parties and have alternate processing site agreement in place and update the contingency plans and system security plans.
4. Identify the cause for backups not being performed and implement a backup schedule in accordance with GSA policy.

3. Risk Management

While performing our FISMA evaluation procedures we inspected various entity-level policy and procedural guides and system security plans, conducted inquiries with individuals to walk through the process and determined that GSA has implemented these policy and procedural guides, however we did identify the following exceptions:

- a. We inspected 19 IT Security Policy/Procedural Guides and determined the following four have not been reviewed or updated annually:
 - IT Security Procedural Guide: Configuration Management (CM) CIO-IT Security-01-05
 - IT Security Procedural Guide: Contingency Planning (CP) CIO-IT Security-06-29
 - IT Security Procedural Guide: Managing Enterprise Risk, CIO-IT Security-06-30
 - IT Security Procedural Guide: Windows 7 Hardening CIO-IT Security-11-61
- b. System security plans for four of the five systems tested were based on NIST SP 800-53, Revision 3, but they should have followed Revision 4.
- c. The Limited Authority to Operate (LATO) for one of five systems expired and the system operated for 23 days until Authority To Operate (ATO) was granted.

NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, “PM-1 Information Security Program Plan” section states:

“The organization:

- a. Develops and disseminates an organization-wide information security program plan that:
 1. Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements;
 2. Includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance;
 3. Reflects coordination among organizational entities responsible for the different aspects of information security (i.e., technical, physical, personnel, cyberphysical); and
 4. Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations and the Nation.
- b. Reviews the organization-wide information security program plan;
- c. Updates the plan to address organizational changes and problems identified during plan implementation or security control assessments; and
- d. Protects the information security program plan from unauthorized disclosure and modification.”

FY 2015 Inspector General Federal Information Security Modernization Act Reporting Metrics, dated June 19, 2015 pages 2-3, states:

“For operational information systems, Department’s or Agency’s (D/A) are expected to be in compliance with NIST guidelines within one year of the publication date.”

GSA Order CIO P 2100.1I - *GSA Information Technology (IT) Security Policy*, October 20, 2014, page 6, states:

“IT security controls. All IT systems, including those operated by a contractor on behalf of the government, must implement proper security controls according to their security categorization level in accordance with Federal Information Processing Standards (FIPS) Publication (PUB) 200, ‘Minimum Security Requirements for Federal Information and Information Systems,’ the current version of NIST SP 800-53, ‘Recommended Security Controls for Federal Information Systems,’ and FIPS PUB 199, ‘Standards for Security Categorization of Federal Information and Information Systems.’”

The NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, CA-6 Security Authorization, pg. F-60 states:

“The organization:

1. Assigns a senior-level executive or manager as the authorizing official for the information system;
2. Ensures that the authorizing official authorizes the information system for processing before commencing operations; and
3. Updates the security authorization [Assignment: *organization-defined frequency*].”

The consolidation of all IT systems into the GSA IT division delayed the review of the IT Security Procedural Guides. This consolidation created the Information Systems Policy and Information Systems Engineering departments, which are responsible for reviewing the IT Security Procedural Guides for the following: Configuration Management, Contingency Planning, Managing Enterprise Risk, and Windows 7 Hardening and are currently undergoing review and updates to be transitioned to NIST 800-53, Rev 4.

The GSA Chief Information Security Officer (CISO) also informed us that due to cost and labor concerns, his office issued guidance which allowed system owners to update their system security plans to be in-accordance with NIST SP 800-53, Revision 4, during their next ATO cycle.

The system’s Security Controls Assessment was not completed and reviewed by GSA management timely. The delay with the completion of the ATO process for system did not allow for the full three year ATO to be signed prior to the expiration of the LATO.

Failing to document an up-to-date IT Security Procedural Guides and system security plans may have a negative effect on subsequent security activities. Specifically, the system owners may not be able to implement, assess, authorize, and monitor the security controls properly for the selected systems; therefore, the system security controls may not be sufficient to protect the confidentiality, integrity, and availability of sensitive information.

Without authorizing a system, the risk associated with that system is accepted. Without authorizations for system use, system owners and management may not be aware of the security risks posed by the use of their systems. As a result, there is the potential that systems are operating in a production environment without appropriate controls or management’s understanding of the system risks. This could further lead to a compromise of the confidentiality, integrity, and availability of the data residing on the information system.

We recommend that GSA perform the following actions:

1. For the four information systems, review and update the system security plans to include all relevant controls from NIST SP 800-53, Revision 4.
2. Continue to review and update the IT Security Procedural Guides to reflect the NIST SP 800-53, Revision 4 security controls.
3. For all other information systems that do not have system security plans that do not include all relevant controls from NIST SP 800-53, Revision 4 formally document this on respective system's and entity wide plan of action and milestones.
4. Provide periodic training over the review and completion of the GSA Authorization package, to include all documents within the enclosure of the package.

4. Security Training

While performing our FISMA evaluation procedures we inspected GSA's security training policy and procedural guides and conducted inquiries with individuals to walk through the security training program. We selected 15 individuals to review their training records and determined that evidence for four individuals could not be provided for role-based training.

The NIST SP 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, AT-3, Role Based Security Training, AT-3, page F-38, states:

“The organization provides role-based security training to personnel with assigned security roles and responsibilities:

- a. Before authorizing access to the information system or performing assigned duties.”

GSA Order CIO P 2100.1I - GSA IT Security Policy, October 20, 2014, page 29, states:

1. “All GSA employees and contractors (internal and external), who have significant information security responsibilities as defined by Office of Personnel Management (OPM) 5 CFR Part 930 and GSA IT security training policy, must complete specialized IT security training as defined in the policy.”

GSA Order CIO 2100.3B Mandatory IT Security Training Requirement for Agency and Contractor Employees with Significant Security Responsibilities, August 13, 2012, page 1, states:

5. “Policy statement. Individuals who hold a position defined within any of the OPM roles described below are required to fulfill all the training requirements identified for that role within ninety (90) days of assignment and every three (3) years thereafter.
 - a. Executives must receive training in information security basics and policy level training in security planning and management. GSA has determined that this role includes all AO who are the executives that accept risk for all IT systems. Executives must complete at least one (1) hour of training by either completing one course from GSA Online University (OLU) as documented in the IT Security Procedural Guide: IT Security Training and Awareness Program CIO IT Security 05-29 or in person training provided by the Senior Agency Information Security Officer (SAISO) on emerging threats and/or security best practices.
 - b. Program and functional managers must receive training in information security basics; management and implementation level training in security planning and system/application security management; and management and implementation level training in system/application life cycle management, risk management, and contingency planning. GSA has determined that these roles include all personnel listed as system program managers/system owners on the IT Security Points of Contact (POC) list. These managers must complete at least six (6) hours of training over a period of three (3) years by either completing courses from OLU and/or an in-person OSAISO approved class, as documented in the IT Security Procedural Guide: IT Security Training and Awareness Program CIO IT Security 05-29.
 - c. CIOs must receive training in information security basics and policy level training in security planning and management. GSA has determined that the CIO role is the same as the AO role. The CIO training requirement will be identical to that for the AOs noted above.

- d. IT Security Program Managers and other security oriented personnel must receive training in information security basics and broad training in security planning, system and application security management, system/application life cycle management, risk management, and contingency planning. GSA has determined these roles to be the ISSM, ISSOs, and regional ISSOs as defined in the IT Security POC list. SSMs and ISSOs (including regional ISSOs) must complete at least sixteen (16) hours of training over a period of three (3) years by either completing courses from OLU and/or in person OSAISO approved class training as documented in the IT Security Procedural Guide: IT Security Training and Awareness Program CIO IT Security 05-29.”

The Office of the Chief Information Officer’s (OCIO) current tracking procedures does not consolidate the tracking of classes users completed, and evidence of successful completion, into their records management sufficiently to demonstrate completion of role based training.

The ineffective monitoring and tracking of role based training records may lead to users not completing training timely as there might be confusion about the user’s current compliance status.

We recommend that GSA perform the following actions:

1. Develop tracking procedures that cohesively tracks the class participation and successful completion of their classes.

5. Plan of Action and Milestones

While performing our FISMA evaluation procedures we inspected GSA's POA&M policy and procedural guides and conducted inquiries with individuals to walk through the POA&M process. We then inspected the POA&Ms and determined that costs associated with weaknesses were not being recorded or tracked for two of the five systems.

NIST SP 800-53, Rev.4, Control CA-5 Plan of Action and Milestones, page F-59, states that:

“The organization:

- a. Develops a plan of action and milestones for the information system to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and
- b. Updates existing plan of action and milestones [*Assignment: organization-defined frequency*] based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.”

The GSA IT Security Procedural Guide: POA&M CIO-IT Security-09-44, on page 4, in Introduction, it states POA&Ms must:

“Be tied to the agency's budget submission through the unique project identifier of a system. This links the security costs for a system with the security performance of a system.”

We were informed by the ISSOs that it was too difficult for GSA IT support personnel to determine cost information for the POA&M weaknesses on an individual basis.

Failure to complete an estimate for the system's POA&M program can result in a lack of available budget for remediating security risk and vulnerabilities.

We recommend that GSA perform the following actions:

1. Tie the agency's budget submission using the systems unique project identifier. This links the security costs for a system with the security performance of a system.
2. Identify, estimate, and record the cost to mitigate weaknesses on the POA&M.

MANAGEMENT RESPONSE TO THE REPORT

The following is the GSA CIO's response, dated October 30, 2015, to the FY 2015 FISMA Evaluation Report.



October 30, 2015

MEMORANDUM FOR CAROLYN PRESLEY-DOSS
DEPUTY ASSISTANT INSPECTOR GENERAL FOR
AUDIT POLICY AND OVERSIGHT (JA)

FROM: DAVID SHIVE 
CHIEF INFORMATION OFFICER (I)

SUBJECT: Agency Management Response - Draft Evaluation Reports:
KPMG's Fiscal Year 2015 Independent Evaluation of the
U.S. General Services Administration's Compliance with the
Federal Information Security Modernization Act of 2014.

The Office of the Chief Information Officer appreciates the opportunity to review and comment on the draft evaluation reports entitled Draft Evaluation Reports: KPMG's Fiscal Year 2015 Independent Evaluation of the U.S. General Services Administration's Compliance with the Federal Information Security Modernization Act of 2014.

We have reviewed the draft evaluation report and we agree with the findings and recommendations stated in the report.

If you have any questions, please contact Kurt Garbars, Chief Information Security Officer (IS), on 202-208-7485.

APPENDIX I – OBJECTIVE, SCOPE, AND METHODOLOGY

The objective for this FISMA evaluation was to conduct an independent evaluation of the information security program and practices of GSA to assess the effectiveness of such programs and practices for the year ending September 30, 2015. Specifically, the objectives of this evaluation are to:

- Perform the annual independent FISMA evaluation of the GSA’s information security programs and practices.
- Respond to DHS FISMA questions on behalf of the GSA Office of Inspector General (OIG).
- Follow up on the status of prior-year FISMA findings.

We conducted our independent evaluation in accordance with the Council of the Inspectors General on Integrity and Efficiency’s Quality Standards for Inspection and Evaluation.

To accomplish our objectives, we evaluated security controls in accordance with applicable legislation, Presidential directives, and the DHS *FY 2015 Inspector General Federal Information Security Modernization Act Reporting Metrics*, dated June 19, 2015. We reviewed the GSA information security program for a program-level perspective and then examined how each of the information systems selected for our testing sample complied with the implementation of these policies and procedures.

We tested a sample of five GSA information systems and five GSA contractor information systems from a total population of 123 major applications and general support systems as of May 11, 2015. We tested the ten information systems to assess whether GSA was effective in implementing the security program and meeting the Federal Information Processing Standards (FIPS) 200 minimum-security standards to protect information and information systems. Five were GSA operated information systems and five were contractor operated information systems.

We mapped the requirements of FY2015 DHS/OMB questions and the top 20 Critical Security Controls for Effective Cyber Defense to the NIST SP 800-53, Revision 4 security controls. The goal of the Critical Controls is to strengthen the defensive posture of GSA’s information security; reduce compromises, recovery efforts, and associated costs; and protect critical assets and infrastructure. The Controls provide continuous, automated monitoring of the most at risk portions of GSA’s information technology infrastructure. Having them in place will allow GSA to focus on its primary mission.

To assess the effectiveness of the information security program and practices of the GSA, our scope included the following:

- Conducting inquiries of information system owners, ISSOs, ISSMs, system administrators and other relevant individuals to walk through each control process.
- An inspection of the information security practices and policies established by the Office of GSA IT.
- An inspection of the information security practices, policies, and procedures in use across GSA

We performed our fieldwork at the GSA’s headquarters offices in Washington, D.C. during the period of April 8, 2015 through August 28, 2015. During our evaluation, we met with GSA management to discuss our preliminary conclusions.

Criteria

We focused our FISMA evaluation approach on federal information security guidance developed by NIST and OMB. NIST Special Publications provide guidelines that are considered essential to the development and implementation of agencies’ security programs. The following is a listing of the criteria used in the performance of the fiscal year (FY) 2015 FISMA evaluation:

NIST, FIPS and/or Special Publications²

- *FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems*
- *FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems*
- *NIST Special Publication 800-16, Information Technology Security Training Requirements: A Role- and Performance-based Model*
- *NIST Special Publication 800-18 Revision 1, Guide for Developing Security Plans for Federal Information Systems*
- *NIST Special Publication 800-30, Guide for Conducting Risk Assessments*
- *NIST Special Publication 800-34 Revision 1, Contingency Planning Guide for Federal Information Systems*
- *NIST Special Publication 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*
- *NIST Special Publication 800-46 Revision 1, Guide to Enterprise Telework and Remote Access Security*
- *NIST Special Publication 800-50, Building an Information Technology Security Awareness and Training Program*
- *NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations*
- *NIST Special Publication 800-53A Revision 1, Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans*
- *NIST Special Publication 800-60 Revision 1, Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories*
- *NIST Special Publication 800-61 Revision 2, Computer Security Incident Handling Guide*
- *NIST Special Publication 800-63-2, Electronic Authentication Guideline*
- *NIST Special Publication 800-70 Revision 2, National Checklist Program for IT Products: Guidelines for Checklist Users and Developers*

OMB Policy Directives

- *OMB Circular A-130, Management of Federal Information Resources*
- *OMB Memorandum 15-01, Fiscal Year 2014 – 2015 Guidance on Improving Federal Information Security and Privacy Management Practices*
- *OMB Memorandum 07-18, Ensuring New Acquisitions Include Common Security Configurations*
- *OMB Memorandum 07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information*
- *OMB Memorandum 07-11, Implementation of Commonly Accepted Security Configurations for Windows Operating Systems*
- *OMB Memorandum 06-19, Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*
- *OMB Memorandum 06-16, Protection of Sensitive Agency Information*
- *OMB Memorandum 05-24, Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors*

² Per OMB FISMA reporting instructions, while agencies are required to follow NIST standards and guidance in accordance with OMB policy, there is flexibility within NIST's guidance documents (specifically in the 800 series) in how agencies apply the guidance. However, NIST FIPS are mandatory. Unless specified by additional implementing policy by OMB, guidance documents published by NIST generally allow agencies latitude in their application. Consequently, the application of NIST guidance by agencies can result in different security solutions that are equally acceptable and compliant with the guidance.

- *OMB Memorandum 04-25, FY 2004 Reporting Instructions for the Federal Information Security Management Act (as amended)*

United States Department of Homeland Security

- *FY 2015 Inspector General Federal Information Security Modernization Act Reporting Metrics*

GSA Policy and Procedural Guides

- *IT Security Procedural Guide: Termination and Transfer CIO-IT Security-03-23, Revision 3, June 30 2015*
- *IT Security Procedural Guide: Access Control CIO-IT Security-01-07, Revision 3, April 1 2015*
- *IT Security Procedural Guide: Audit and Accountability CIO-IT Security-01-08, Revision 3, June 30 2010*
- *IT Security Procedural Guide: Configuration Management CIO-IT Security-01-05, Revision 2, March 22 2010*
- *IT Security Procedural Guide: Information Security Program Plan, Version 1.0, May 1 2015*
- *IT Security Procedural Guide: Contingency Planning CIO-IT Security-06-29, Revision 2, August 16 2010*
- *IT Security Procedural Guide: Plan of Action and Milestones (POA&M) CIO-IT Security-09-44, May 17 2013*
- *IT Security Procedural Guide: CIO-IT Security-09-48 Security Language for IT Acquisition Efforts, Revision 2, November 7 2014*
- *GSA IT Security Policy, CIO P 2100.II CHGE 1, October 20 2014*
- *IT Security Procedural Guide: Incident Response, CIO-IT Security-01-02, Revision 9, April 7 2015*
- *IT Security Procedural Guide: IT Security Procedural Guide: Identification and Authentication, CIO-IT Security-01-01, Revision 4, May 30 2015*
- *IT Security Procedural Guide: IT Security Training and Awareness Program CIO-IT Security 05-29, Revision 4, June 15 2015*
- *IT Security Procedural Guide: Information Security Continuous Monitoring Strategy, CIO-IT Security-12-66IT, April 3 2014*
- *GSA Telecommunications Policy CIO P 2165.2*
- *IT Security Procedural Guide: FY 2015 IT Security Program Management Implementation Plan CIO-IT Security-08-39, Revision 7, October 30 2014*
- *IT Security Procedural Guide: Managing Enterprise Risk Security Assessment and Authorization, Planning, and Risk Assessment (CA, PL, & RA) CIO-IT Security-06-30, Revision 7, May 31 2011*
- *Risk Management Strategy, Version 1.0, June 16 2015*
- *2100.3B CIO Mandatory Information Technology (IT) Security Training Requirement for Agency and Contractor Employees with Significant Security Responsibilities, August 13 2012*
- *(Initial and Annual) Policy and Procedure CIO 2104.1A GSA Information Technology (IT) General Rules of Behavior (5-18-2012) (Revised 2-19-2014)*

APPENDIX II – STATUS OF PRIOR-YEAR FINDINGS

In Fiscal Year (FY) 2014, another firm conducted the FISMA Evaluation. As part of this year’s FISMA Evaluation, we followed up on the status of the prior year findings. We inquired of GSA personnel and inspected evidence to determine the status of the findings. If recommendations were determined to be implemented, we closed the findings. If recommendations were determined to be only partially implemented or not implemented at all, we determined the finding to be open. (Please note that Findings 2.4, 2.5, 2.6 and their recommendations have been redacted due to the sensitive nature of the material; however, we noted that management closed these three findings).

Prior Year Findings – 2014 Evaluation

| Finding # | Prior-Year Condition | Recommendation(s) | Status |
|---|--|--|-----------------------------------|
| <p>2.1 – Organization-wide Security Management Program</p> | <p>GSA has not developed, documented, and implemented an Office of the Chief Information Officer and Office of the Chief Information Security Officer approved organization-wide system security plan.</p> <p>GSA has not designed and implemented a unified set of common and system-specific or hybrid controls. Common controls are security controls that are inheritable by one or more of the organization’s information systems. The organization assigns responsibility for common controls to appropriate organization officials and coordinates the development, implementation, assessment, authorization and monitoring of the controls.</p> <p>The identification of common controls is most effectively accomplished as an organization-wide exercise with the active involvement of the CIO, senior</p> | <p>1. Develop, document, and implement an organization-wide information security program that describes the program management controls and common controls in place or plan for meeting the security requirements for individual information systems and the totality of information technology assets, data, and security controls supporting GSA’s organizational mission.</p> <p>2. Complete the selection, design and implementation of common controls, as system specific or hybrid controls, on an organization-wide basis with the involvement of the organization’s senior leadership. Mandate that all Service and Staff Offices (S/SO) (federally and contractor-managed) identify within their system security plans, which controls are inherited as system specific, which are shared</p> | <p>1. Closed</p> <p>2. Closed</p> |

| Finding # | Prior-Year Condition | Recommendation(s) | Status |
|-----------|--|--|---------------------------------|
| | <p>information security officer, risk executive (function), authorizing officials, information system owners, information owners/stewards, and information system security officers.</p> <p>Security controls not designated as common controls are considered system-specific or hybrid controls. System-specific controls are the primary responsibility of information system owners and their respective authorizing officials. Organizations assign a hybrid status to a security control when one part of the control is deemed to be common and another part of the control is deemed to be system-specific.</p> <p>Partitioning security controls into common, hybrid, and system-specific controls can result in significant savings to the organization in implementation and assessment costs, as well as a more consistent application of the security controls across the organization.</p> <p>While the concept of security control partitioning into common, hybrid, and system specific controls is straightforward and intuitive, the application within an organization takes significant planning and coordination.</p> <p>GSA has not implemented a process to maintain POA&Ms for the organization-</p> | <p>responsibilities as hybrid controls, and which are S/SO application-specific responsibilities. Hold S/SO accountable and monitor their performance and compliance through GSA monitoring and reporting channels and processes. Ensure that compliance with the organization-wide implementation of common, hybrid, and application specific controls are made a requirement over time in all contracting vehicles standard language.</p> <p>3. Implement a process to maintain POA&Ms for organization-wide information security program performance, in accordance with NIST 800-53, Revision 4.</p> <p>4. Develop, document, and implement an organization-wide risk management strategy that includes a clear expression of the risk tolerance for the organization; acceptable risk assessment methodologies; risk mitigation strategies; the organization's defined metrics for acceptable risk tolerance; and approaches for monitoring risk over time.</p> | <p>3.Closed</p> <p>4.Closed</p> |

| Finding # | Prior-Year Condition | Recommendation(s) | Status |
|-----------|---|-------------------|--------|
| | <p>wide information security program performance; however, GSA does have a process to maintain POA&Ms for the FISMA reportable systems. Lack of organization-wide information security program management controls, such as organization-wide POA&Ms, results in the risk that there is an inconsistency in the design and implementation of the organization-wide information security program. The risk of inconsistency in the implementation of information security program management controls increases the exposure that FISMA controls are either over applied or under applied. This may result in potential gaps (vulnerabilities) in the enterprise security posture, which could provide additional vectors or gaps for threat agents to exploit.</p> <p>GSA has not developed, documented, and implemented a comprehensive strategy to manage risk to organizational operations and assets, individuals, and other stakeholders; nor has it implemented any strategy consistently across the organization. An organization-wide risk management strategy includes, for example, a clear expression of the risk tolerance for the organization, acceptable risk assessment methodologies, risk mitigation strategies, the organization's defined metrics for acceptable risk</p> | | |

| Finding # | Prior-Year Condition | Recommendation(s) | Status |
|---|---|--|--|
| | tolerance, and approaches for monitoring risk over time. | | |
| 2.2 – Configuration-Related Vulnerabilities | While performing our FISMA evaluation procedures, we determined that GSA has not documented the timely remediation of configuration-related vulnerabilities, including scan findings, as part of the POA&M process, as specified in the organization’s policies and procedures. In accordance with GSA guidelines, “GSA requires the mitigation of all HIGH RISK vulnerabilities within 30 days (of identifying vulnerabilities) per the Government Performance and Results Act measures.” However, GSA does not have organization-wide policies and procedures for determining whether the organization remediates high risk vulnerabilities within a timely manner. | <ol style="list-style-type: none"> 1. Develop policies and procedures that require retention of the dates for remediating vulnerabilities resulting from the scans. 2. Develop procedures to determine whether configuration-related vulnerabilities are remediated within a timely manner of the weaknesses discovery. | <ol style="list-style-type: none"> 1. Closed 2. Open |
| 2.3 – Identification and Authentication and Access Control Policies and Procedures | <p>Inspection of the identification and authentication and access control policies and procedures revealed the following:</p> <ul style="list-style-type: none"> • GSA IT Security Procedural Guide: Identification and Authentication (IA) CIO-IT Security-01-01 is dated June 22, 2010 and does not address current operating systems such as Windows 7 or later versions. • GSA IT Security Procedural Guide: Access Control CIO-IT Security-01-07 is dated January 30, 2008 and does not address executive orders issued since 2008 and current policies and | <ol style="list-style-type: none"> 1. Review and update the current: <ol style="list-style-type: none"> a. Identification and authentication policies; and b. Identification and authentication procedures. 2. Review and update the current: <ol style="list-style-type: none"> a. Access control policies; and b. Access control procedures. | <ol style="list-style-type: none"> 1. Closed 2. Closed |

| Finding # | Prior-Year Condition | Recommendation(s) | Status |
|-----------|--|-------------------|--------|
| | <p>procedures.</p> <ul style="list-style-type: none"> GSA IT Security Procedural Guide: Termination and Transfer CIO-IT Security-03-23 is dated January 29, 2008 and may not reflect current policies and procedures. <p>These documents are designed to address the establishment of GSA policies and procedures for effective implementation of selected security controls and control enhancements in the “Identification and Authentication” and “Access Control” families. Therefore, policies and procedure guides should be reviewed and updated at least annually to reflect applicable current federal laws, Executive Orders, directives, regulations, policies, standards, and guidance.</p> | | |

APPENDIX III – GLOSSARY

| ACRONYM | DEFINITION |
|----------------|--|
| AO | Authorizing Officials |
| ATO | Authority To Operate |
| CIO | Chief Information Officer |
| CISO | Chief Information Security Officer |
| CM | Configuration Management |
| CP | Contingency Planning |
| D/A | Department or Agency |
| DHS | Department of Homeland Security |
| FIPS | Federal Information Processing Standards |
| FISMA | Federal Information Security Modernization Act |
| FY | Fiscal Year |
| GSA | U.S. General Services Administration |
| IA | Identification and Authentication |
| IG | Inspector General |
| ISSM | Information System Security Manager |
| ISSO | Information System Security Officer |
| IT | Information Technology |
| LATO | Limited Authority to Operate |
| NIST | National Institute of Standards and Technology |
| OCISO | Office of the Chief Information Officer |
| OIG | Office of Inspector General |
| OLU | Online University |
| OMB | Office of Management and Budget |
| OPM | Office of Personnel Management |
| POA&M | Plan of Action and Milestones |
| SAISO | Senior Agency Information Security Officer |
| S/SO | Service and Staff Offices |
| SP | Special Publication |