



Office of Audits
Office of Inspector General
U.S. General Services Administration

Independent Evaluation of the
U.S. General Services Administration
Compliance with the Federal Information
Security Management Act of 2002 for
Fiscal Year 2014

*Assignment Number A140022
November 18, 2014*


NOTICE

Sections of this report have been redacted due to the sensitive nature of the material.



U.S. GENERAL SERVICES ADMINISTRATION
Office of Inspector General

NOV 18 2014

MEMORANDUM FOR: DANIEL M. TANGHERLINI
ADMINISTRATOR (A)

FROM: ROBERT C. ERICKSON, JR.
DEPUTY INSPECTOR GENERAL (J)
SUBJECT: Transmittal of the Independent Evaluation of the U.S.
General Services Administration Compliance with the
Federal Information Security Management Act of
2002 For Fiscal Year 2014
Assignment Number A140022

Attached are the results of the evaluation of GSA's compliance with the *Federal Information Security Management Act of 2002* (FISMA) for fiscal year 2014 conducted by Brown & Company CPAs, PLLC (Brown & Company).

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. The GSA OIG determined that a contractor would perform the annual evaluation for GSA. Therefore, GSA contracted with the independent public accounting firm, Brown & Company, to assess its information security program in accordance with FISMA for fiscal year 2014.

Brown & Company is responsible for the findings and recommendations included in the report. We do not express an opinion on the effectiveness of GSA's information security controls during fiscal year 2014. The Office of the Chief Information Officer and the Office of Mission Assurance response to the draft report is included in its entirety as an appendix.

In fiscal year 2015, the 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 Brown & Company 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

1800 F Street, NW, Washington, DC 20405-0002

Federal Recycling Program



Printed on Recycled Paper

**Independent Evaluation of the
U. S. General Services Administration
Compliance with Provisions of the
Federal Information Security Management Act of 2002 (FISMA)**

For Fiscal Year 2014

Prepared by:

Brown & Company CPAs, PLLC
Certified Public Accountants and Management Consultants
1101 Mercantile Lane, Suite 122
Largo, Maryland 20774
(240) 770-4900

Date: October 28, 2014



BROWN & COMPANY CPAs, PLLC
CERTIFIED PUBLIC ACCOUNTANTS AND MANAGEMENT CONSULTANTS

**Independent Evaluation of the
U. S. General Services Administration
Compliance with Provisions of the
Federal Information Security Management Act of 2002 (FISMA)**

Administrator and Acting Inspector General
United States General Services Administration:

Brown & Company CPAs, PLLC (Brown & Company) is pleased to submit this report in support of evaluation services provided pursuant to requirements of the Federal Information Security Management Act of 2002 (FISMA). Brown & Company conducted an independent evaluation of the United States General Services Administration's information security program for the fiscal year (FY) ended September 30, 2014. The FISMA evaluation was performed from June 13, 2014 to September 29, 2014.

We conducted the FISMA evaluation in accordance with the President's Council on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation*, issued January 2012 and subsequent revisions and in compliance with the Inspector General Reform Act of 2008 and Office of Management and Budget's most recent FISMA reporting guidance. These standards require that we plan and perform the evaluation to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our evaluation objectives. We believe that the evidence we obtained provides a reasonable basis for our findings and conclusions based on the evaluation objectives.

Largo, Maryland
October 28, 2014

**Independent Evaluation of the
U. S. General Services Administration
Compliance with Provisions of the
Federal Information Security Management Act of 2002 (FISMA)
For Fiscal Year 2014**

Table of Contents

1	Executive Summary	1
2	Evaluation Procedures, Results and Findings.....	2
2.1	Organization-wide Security Management Program.....	2
2.2	Configuration-Related Vulnerabilities	6
2.3	Identification and Authentication and Access Control Policies and Procedures	7
2.4	8
2.5	9
2.6	10
3	Recommendations	11
3.1	Organization-wide Security Management Program.....	11
3.2	Configuration-Related Vulnerabilities	12
3.3	Identification and Authentication and Access Control Policies and Procedures	12
3.4	12
3.5	13
3.6	13
4	Management Comments.....	13
5	Conclusion	13
Appendices.....		A-1
	Appendix A – Purpose, Scope, and Methodology.....	A-1
	Appendix B – Management Comments.....	B-1
	Appendix C – FY 2014 Inspector General FISMA Reporting Metrics	C-1



1 Executive Summary

The United States General Services Administration (GSA) contracted with Brown & Company CPAs, PLLC (Brown & Company) to conduct an Independent Evaluation of GSA's compliance with the provisions of the Federal Information Security Management Act of 2002 (FISMA). FISMA requires agencies to develop, document, and implement an organization-wide information security program to provide 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.

GSA's information security program provides guidance and oversight to protect GSA systems and data. The purpose of the independent evaluation is to determine if GSA's information security program meets the requirements of FISMA.

In assessing GSA's adherence to FISMA, the following areas were reviewed:

- 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
- Contractor Systems
- Security Capital Planning

The objective of this evaluation was to determine if GSA developed, documented, and implemented a comprehensive organization-wide information security program that addresses risks in the current Information Technology (IT) environment. If so, identify additional actions needed to strengthen GSA's information security program and to protect the confidentiality, integrity and availability of GSA's systems and data.

Based on the results of our evaluation, Brown & Company has concluded that GSA has made positive strides over the last year in addressing information security weaknesses and continues to make progress in becoming fully FISMA compliant. However, GSA still faces challenges to fully implement information security requirements as stipulated in federal guidelines and mandates. This report contains findings and recommendations for six areas concerning issues such as:

1. Improvement to the organization-wide security management program including an organization-wide system security plan; a unified set of common and system specific or hybrid controls; a process to maintain plan of action and milestones (POA&M) for an organization-wide security program performance; and an organization-wide risk management strategy.

2. Development of policies and procedures to determine whether or not configuration-related vulnerabilities are remediated within a timely manner.
3. Updates to the identification and authentication and access control policies and procedures.
4. [REDACTED]
5. [REDACTED]
6. [REDACTED]

This report presents results for the FY 2014 evaluation of GSA's information security program and reflects results from evaluations conducted by Brown & Company on five selected systems.

2 Evaluation Procedures, Results and Findings

2.1 Organization-wide Security Management Program

While performing our FISMA evaluation procedures, we determined that GSA has implemented numerous elements of an organization-wide security management program. However, after interviewing personnel, inspecting documentation, and observing operations and process walkthroughs, we have determined that certain key elements have not been developed, documented, and implemented. These key elements are discussed below.

1. 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.
2. 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. The identification of common controls is most effectively accomplished as an organization-wide exercise with the active involvement of the Chief Information Officer (CIO), senior information security officer, risk executive (function), authorizing officials, information system owners, information owners/stewards, and information system security officers.

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.

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. 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.

3. GSA has not implemented a process to maintain POA&Ms for the organization-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.
4. 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 tolerance, and approaches for monitoring risk over time.

National Institute of Standards and Technology (NIST) Special Publication (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, cyber-physical); 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.

Supplemental Guidance: Information security program plans can be represented in single documents or compilations of documents at the discretion of the organization. The plans document the program management controls and organization-defined common controls. Information security program plans provide sufficient information about the program management controls/common controls (including specification of parameters for any *assignment* and *selection* statements either explicitly or by reference) to enable implementations that are unambiguously compliant with the intent of the plans and a determination of the risk to be incurred if the plans are implemented as intended.

The security plans for individual information systems and the organization-wide information security program plan together provide complete coverage for all security controls employed within the organization. Common controls are documented in an appendix to the organization's information security program plan unless the controls are included in a separate security plan for an information system (e.g., security controls employed as part of an intrusion detection system providing organization-wide boundary protection inherited by one or more organizational information systems). The organization-wide information security program plan will indicate which separate security plans contain descriptions of common controls.

NIST Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, PM-4 "Plan of Action and Milestones Process" section states:

The organization:

- a. Implements a process for ensuring that plans of action and milestones for the security program and associated organizational information systems:
 - 1. Are developed and maintained;
 - 2. Document the remedial information security actions to adequately respond to risk to organizational operations and assets, individuals, other organizations, and the Nation; and
 - 3. Are reported in accordance with Office of Management and Budget (OMB) FISMA reporting requirements.
- b. Reviews plans of action and milestones for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.

Supplemental Guidance: The plan of action and milestones is a key document in the information security program and is subject to federal reporting requirements established by OMB. With the increasing emphasis on organization-wide risk management across all three tiers in the risk management hierarchy (i.e., organization, mission/business process,

and information system), organizations view plans of action and milestones from an organizational perspective, prioritizing risk response actions and ensuring consistency with the goals and objectives of the organization.

NIST Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, “PM-9 Risk Management Strategy” section states:

The organization:

- a. Develops a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of information systems;
- b. Implements the risk management strategy consistently across the organization; and
- c. Reviews and updates the risk management strategy as required, to address organizational changes.

Supplemental Guidance: An organization-wide risk management strategy includes, for example, an unambiguous expression of the risk tolerance for the organization, acceptable risk assessment methodologies, risk mitigation strategies, a process for consistently evaluating risk across the organization with respect to the organization’s risk tolerance, and approaches for monitoring risk over time.

Because GSA has not completed the implementation of its organization-wide information security program plan, it has not performed security assessment procedures for organization-wide common and hybrid controls. Without assessment results for organization-wide controls, GSA does not have the vulnerability data required to process and maintain organization-wide security program performance POA&Ms for organization-wide controls weakness remediation.

Risk assessments can be conducted at all three tiers in the risk management hierarchy—including Tier 1 (organization level), Tier 2 (mission/business process level), and Tier 3 (information system level). While performing the FISMA procedures, we noted GSA documentation that supports the performance of risk management activities related to Tier 3, and to a limited extent, Tier 2 strategic objectives and activities. However, we did not note any examples of GSA’s current performance of risk assessments at the Tier 1 level as described in NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*.

Lack of organization-wide security program management controls results in the risk that there is an inconsistency in the design and implementation of the organization-wide security program. The risk of inconsistency in the implementation of 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 for threat agents to exploit gaps within the controls over federally managed and / or contractor managed information systems.

The effect of not designing and implementing an organization-wide risk management plan and assessment is that GSA’s responsible personnel may not be kept abreast adequately or in a timely manner, of organization-wide threats, vulnerabilities, and attack vectors. Organization-wide

threats, vulnerabilities, and attack vectors may not be apparent solely from analysis of individual risk management plans and assessment results for FISMA reportable systems (i.e. general support systems, major and minor applications with consolidated analytics for identification of systemic risks).

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 or not the organization remediates high risk vulnerabilities within a timely manner.

NIST Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, "RA-5 Vulnerability Scanning" section states:

The organization:

- a. Scans for vulnerabilities in the information system and hosted applications in accordance with organization-defined process and when new vulnerabilities potentially affecting the system/applications are identified and reported;
- b. Employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:
 1. Enumerating platforms, software flaws, and improper configurations;
 2. Formatting checklists and test procedures; and
 3. Measuring vulnerability impact.
- c. Analyzes vulnerability scan reports and results from security control assessments;
- d. Remediates legitimate vulnerabilities in defined response times in accordance with an organizational assessment of risk; and
- e. Shares information obtained from the vulnerability scanning process and security control assessments with defined personnel or roles to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

In accordance with GSA's *IT Security Procedural Guide*, Revision 1, dated November 03, 2010: Plan of Action and Milestones CIO-IT-Security-09-44, POA&Ms must include all known IT security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency. POA&Ms shall be developed within a timely manner of the weakness discovery. Specifically, the "POA&M Weakness Tracking Requirements" section of the guide states:

“Vulnerability Scanning. Include all vulnerabilities identified from operating system vulnerability scans in the POA&M. All systems must be scanned at least quarterly. Vulnerabilities resulting from scans must be added to the POA&M and scan reports submitted together with the quarterly POA&M update. GSA requires the mitigation of all HIGH RISK vulnerabilities within 30 days (of identifying vulnerabilities) per the Government Performance and Results Act (GPRA) measures.”

The weakness exists because GSA’s policies and procedures do not require retention of the dates for remediating vulnerabilities resulting from vulnerability scans. GSA utilizes a vulnerability tracking system that maintains information on the remediation of configuration-related vulnerabilities for the FISMA reportable systems; however, GSA has not developed procedures to determine if high risk vulnerabilities are remediated within 30 days.

The effect of the lack of policies and procedures to determine if the organization mitigates high risk vulnerabilities in a timely manner increases the risk that GSA will not remediate legitimate vulnerabilities in accordance with GSA’s assessment of risk.

2.3 Identification and Authentication and Access Control Policies and Procedures

While performing our FISMA evaluation procedures, we determined that GSA has implemented some elements of its “Identification and Authentication” and “Access Control” families. However, after interviewing personnel, inspecting documentation, and observing operations and process walkthroughs, we have determined that certain identification and authentication and access control policies and procedures have not been reviewed and updated.

1. Inspection of the identification and authentication and access control policies and procedures revealed the following:
 - *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 procedures.
 - *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.

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.

NIST Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, “IA-1 Identification and Authentication Policy and Procedures” section states:

The organization:

- a. Develops, documents, and disseminates to personnel:
 - 1. An identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
 - 2. Procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls; and
- b. Reviews and updates the current:
 - 1. Identification and authentication policy and
 - 2. Identification and authentication procedures.

Section “AC-1 Access Control Policy and Procedures” states:

The organization:

- a. Develops, documents, and disseminates to personnel:
 - 1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
 - 2. Procedures to facilitate the implementation of the access control policy and associated access controls; and
- b. Reviews and updates the current:
 - 1. Access control policy; and
 - 2. Access control procedures.

The weakness exists because the GSA Policy and Compliance Division, Office of the Chief Information Security Officer, has not fully implemented GSA’s FY 2014 Security and Privacy Project Plan which includes updating several information security policies and procedures by first quarter FY 2015.

The effect of not reviewing and updating information system security control policies and procedures increases the risk of unauthorized access to GSA information and information systems.

2.4

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

2.5 [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

2.6 [REDACTED]

[REDACTED]

[REDACTED]

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.

3. Implement a process to maintain POA&Ms for organization-wide information security program performance, in accordance with NIST 800-53, Revision 4.
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.

3.2 Configuration-Related Vulnerabilities

1. Develop policies and procedures that require retention of the dates for remediating vulnerabilities resulting from the scans.
2. Develop procedures to determine whether or not configuration-related vulnerabilities are remediated within a timely manner of the weaknesses discovery.

3.3 Identification and Authentication and Access Control Policies and Procedures

1. Review and update the current:
 - a. Identification and authentication policies; and
 - b. Identification and authentication procedures.
2. Review and update the current:
 - a. Access control policies; and
 - b. Access control procedures

3.4

[REDACTED]

3.5 [REDACTED]

[REDACTED]

[REDACTED]

3.6 [REDACTED]

[REDACTED]

4 Management Comments

Management agreed with our findings and recommendations. Complete responses by the Office of the Chief Information Officer and Office of Mission Assurance are presented in **Appendix B**.

5 Conclusion

Given the range of potential security threats, GSA is focusing their information security activity on the most cost-effective and efficient controls relevant for their organizations and related mission needs. GSA is developing strategies, in conjunction with Department of Homeland Security, to improve GSA's information security posture. We found that additional steps are needed to strengthen GSA's information security program in key areas: (1) Organization-wide Security Management Program; (2) Configuration-related Vulnerabilities (3) Identification and Authentication and Access Control Policies and Procedures; (4) [REDACTED] (5) [REDACTED] and (6) [REDACTED]

We believe that making the security improvements recommended in this report will better enable GSA to protect the confidentiality, availability, and integrity of the organization's information and information systems.

Appendices

Appendix A – Purpose, Scope, and Methodology

Purpose

The Federal Information Security Management Act of 2002 (FISMA) requires an annual independent evaluation of the General Services Administration's (GSA) Information Technology (IT) Security Program. To meet the FISMA requirements, Brown & Company conducted an evaluation encompassing assessments of GSA's security program and security controls for select systems.

Scope

The evaluation's scope included assessments of controls for GSA's IT Security Program and reflects results from evaluations of five selected systems conducted throughout the FY 14 FISMA Assessment Period by Brown & Company. In addition, the FISMA evaluation scope included evaluation of the Office of the Chief Information Officer's oversight of IT security control implementation for GSA information and information systems.

Methodology

To accomplish our objectives, Brown & Company:

1. Met with GSA officials in the Office of the Chief Information Officer, Office of Mission Assurance, Federal Acquisition Service, and Public Buildings Service.
2. Applied the NIST Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*.
3. Reviewed applicable information security regulations, policies, and guidance.
4. Evaluated the following FISMA areas:
 - 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
 - Contractor Systems
 - Security Capital Planning

5. Assessed the results of the completed system security reviews for five systems.
6. Conducted site visits and performed on-site FISMA evaluation procedures at government and contractor-managed data centers located in Stennis, Mississippi, and Rockville, Maryland.
7. Performed an assessment of CyberScope questions for five FISMA reportable systems by examining the system assessment and authorization package, including the system risk assessment, security plan, security assessment results, contingency plan, and POA&M.
8. Reviewed the GSA's policies and procedures for remediating configuration-related vulnerabilities.

To determine implementation of certain CyberScope controls, we chose a judgmental sample of five FISMA reportable systems, which included both general support systems and major applications.

We conducted the evaluation between June 13, 2014 and September 29, 2014 in accordance with the President's Council on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation*, issued January 2012 and subsequent revisions, in compliance with the Inspector General Reform Act of 2008, and with OMB's most recent FISMA reporting guidance. Those standards require that we plan and perform the evaluation to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our evaluation objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our evaluation objectives.

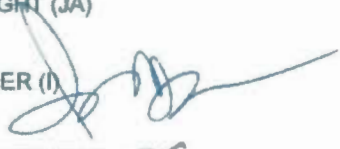
Appendix B – Management Comments




U.S. General Services Administration

October 21, 2014

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

FROM: SONNY HASHMI
CHIEF INFORMATION OFFICER (I) 

ROBERT CARTER
ACTING ASSOCIATE ADMINISTRATOR
OFFICE OF MISSION ASSURANCE (D) 

SUBJECT: Brown and Company's Independent Evaluation of the U.S.
General Services Administration Compliance with Provisions of
the Federal Information Security Management Act of 2002 for
Fiscal Year 2014, Report Number - A140022

The Office of the Chief Information Officer and the Office of Mission Assurance appreciates the opportunity to review and comment on the draft report entitled *Brown and Company's Independent Evaluation of the U.S. General Services Administration Compliance with Provisions of the Federal Information Security Management Act of 2002 for Fiscal Year 2014*.

We have reviewed the draft audit 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.

1800 F Street, NW
Washington, DC 20405
www.gsa.gov

Appendix C - FY 2014 Inspector General FISMA Reporting Metrics

The following pages contain the GSA Inspector General 2014 Annual FISMA Report

Inspector General

Section Report

2014
Annual FISMA
Report

General Services Administration

Section 1: Continuous Monitoring Management

1.1 Has the organization established an enterprise-wide continuous monitoring program that assesses the security state of information systems that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?



Comments:

[Redacted]

1.1.1 Documented policies and procedures for continuous monitoring (NIST SP 800-53: CA-7).



1.1.2 Documented strategy for information security continuous monitoring (ISCM).



1.1.3 Implemented ISCM for information technology assets.



Comments:

[Redacted]

1.1.4 Evaluate risk assessments used to develop their ISCM strategy.



1.1.5 Conduct and report on ISCM results in accordance with their ISCM strategy.



1.1.6 Ongoing assessments of security controls (system-specific, hybrid, and common) that have been performed based on the approved continuous monitoring plans (NIST SP 800-53, 800-53A).



Comments:

[Redacted]

Section 1: Continuous Monitoring Management

1.1.7 Provides authorizing officials and other key system officials with security status reports covering updates to security plans and security assessment reports, as well as a common and consistent POA&M program that is updated with the frequency defined in the strategy and/or plans (NIST SP 800-53, 800-53A).



Comments:



1.2 Please provide any additional information on the effectiveness of the organization's Continuous Monitoring Management Program that was not noted in the questions above.



Section 2: Configuration Management

2.1 Has the organization established a security configuration management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?



Comments:



2.1.1 Documented policies and procedures for configuration management.



2.1.2 Defined standard baseline configurations.



2.1.3 Assessments of compliance with baseline configurations.



Comments:



2.1.4 Process for timely (as specified in organization policy or standards) remediation of scan result deviations.



Section 2: Configuration Management

2.1.5 For Windows-based components, USGCB secure configuration settings are fully implemented, and any deviations from USGCB baseline settings are fully documented.



2.1.6 Documented proposed or actual changes to hardware and software configurations.



2.1.7 Process for timely and secure installation of software patches.



Comments:



2.1.8 Software assessing (scanning) capabilities are fully implemented (NIST SP 800-53: RA-5, SI-2).



2.1.9 Configuration-related vulnerabilities, including scan findings, have been remediated in a timely manner, as specified in organization policy or standards. (NIST SP 800-53: CM-4, CM-6, RA-5, SI-2)



Comments:



2.1.10 Patch management process is fully developed, as specified in organization policy or standards. (NIST SP 800-53: CM-3, SI-2).



Comments:



2.2 Please provide any additional information on the effectiveness of the organization's Configuration Management Program that was not noted in the questions above.



2.3 Does the organization have an enterprise deviation handling process and is it integrated with the automated capability.



Comments:



Section 2: Configuration Management

2.3.1 Is there a process for mitigating the risk introduced by those deviations?



Comments:

[Redacted comment text]

Section 3: Identity and Access Management

3.1 Has the organization established an identity and access management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines and identifies users and network devices? Besides the improvement opportunities that have been identified by the OIG, does the program include the following attributes?



3.1.1 Documented policies and procedures for account and identity management (NIST SP 800-53: AC-1).



Comments:

[Redacted comment text]

3.1.2 Identifies all users, including Federal employees, contractors, and others who access organization systems (NIST SP 800-53, AC-2).



3.1.3 Identifies when special access requirements (e.g., multi-factor authentication) are necessary.



3.1.4 If multi-factor authentication is in use, it is linked to the organization's PIV program where appropriate (NIST SP 800-53, IA-2).



3.1.5 Organization has planned for implementation of PIV for logical access in accordance with government policies (HSPD 12, FIPS 201, OMB M-05-24, OMB M-07-06, OMB M-08-01, OMB M-11-11).



Comments:

[Redacted comment text]

Section 3: Identity and Access Management

- 3.1.6 Organization has adequately planned for implementation of PIV for physical access in accordance with government policies (HSPD 12, FIPS 201, OMB M-05-24, OMB M-07-06, OMB M-08-01, OMB M-11-11).
■
- 3.1.7 Ensures that the users are granted access based on needs and separation-of-duties principles.
■
- 3.1.8 Identifies devices with IP addresses that are attached to the network and distinguishes these devices from users (For example: IP phones, faxes, and printers are examples of devices attached to the network that are distinguishable from desktops, laptops, or servers that have user accounts).
■
- 3.1.9 Identifies all user and non-user accounts. (Refers to user accounts that are on a system. Data user accounts are created to pull generic information from a database or a guest/anonymous account for generic login purposes. They are not associated with a single user or a specific group of users.)
■
- 3.1.10 Ensures that accounts are terminated or deactivated once access is no longer required.
■
- 3.1.11 Identifies and controls use of shared accounts.
■

Comments:

- 3.2 Please provide any additional information on the effectiveness of the organization's Identity and Access Management Program that was not noted in the questions above.
■

Section 4: Incident Response and Reporting

- 4.1 Has the organization established an incident response and reporting program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?
■

Section 4: Incident Response and Reporting

- 4.1.1 Documented policies and procedures for detecting, responding to, and reporting incidents (NIST SP 800-53: IR-1).
■
 - 4.1.2 Comprehensive analysis, validation and documentation of incidents.
■
 - 4.1.3 When applicable, reports to US-CERT within established timeframes (NIST SP 800-53, 800-61, and OMB M-07-16, M-06-19).
■
 - 4.1.4 When applicable, reports to law enforcement within established timeframes (NIST SP 800-61).
■
 - 4.1.5 Responds to and resolves incidents in a timely manner, as specified in organization policy or standards, to minimize further damage (NIST SP 800-53, 800-61, and OMB M-07-16, M-06-19).
■
 - 4.1.6 Is capable of tracking and managing risks in a virtual/cloud environment, if applicable.
■
 - 4.1.7 Is capable of correlating incidents.
■
 - 4.1.8 Has sufficient incident monitoring and detection coverage in accordance with government policies (NIST SP 800-53, 800-61; OMB M-07-16, M-06-19).
■
- 4.2 Please provide any additional information on the effectiveness of the organization's Incident Management Program that was not noted in the questions above.
■

Section 5: Risk Management

- 5.1 Has the organization established a risk management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?
■

Section 5: Risk Management

5.1.1 Documented policies and procedures for risk management, including descriptions of the roles and responsibilities of participants in this process.



5.1.2 Addresses risk from an organization perspective with the development of a comprehensive governance structure and organization-wide risk management strategy as described in NIST SP 800-37, Rev.1.



Comments:

[Redacted comment text]

5.1.3 Addresses risk from a mission and business process perspective and is guided by the risk decisions from an organizational perspective, as described in NIST SP 800-37, Rev. 1.



Comments:

[Redacted comment text]

5.1.4 Addresses risk from an information system perspective and is guided by the risk decisions from an organizational perspective and the mission and business perspective, as described in NIST SP 800-37, Rev. 1.



Comments:

[Redacted comment text]

5.1.5 Has an up-to-date system inventory.



5.1.6 Categorizes information systems in accordance with government policies.



5.1.7 Selects an appropriately tailored set of baseline security controls.



Section 5: Risk Management

- 5.1.8 Implements the tailored set of baseline security controls and describes how the controls are employed within the information system and its environment of operation.
■
- 5.1.9 Assesses the security controls using appropriate assessment procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
■
- 5.1.10 Authorizes information system operation based on a determination of the risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation of the information system and the decision that this risk is acceptable.
■
- 5.1.11 Ensures information security controls are monitored on an ongoing basis, including assessing control effectiveness, documenting changes to the system or its environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to designated organizational officials.
■
- 5.1.12 Information-system-specific risks (tactical), mission/business-specific risks, and organizational-level (strategic) risks are communicated to appropriate levels of the organization.
■
- 5.1.13 Senior officials are briefed on threat activity on a regular basis by appropriate personnel (e.g., CISO).
■
- 5.1.14 Prescribes the active involvement of information system owners and common control providers, chief information officers, senior information security officers, authorizing officials, and other roles as applicable in the ongoing management of information-system-related security risks.
■
- 5.1.15 Security authorization package contains system security plan, security assessment report, and POA&M in accordance with government policies. (NIST SP 800-18, SP 800-37).
■

Section 5: Risk Management

5.1.16 Security authorization package contains accreditation boundaries, defined in accordance with government policies, for organization information systems.



5.2 Please provide any additional information on the effectiveness of the organization's Risk Management Program that was not noted in the questions above.



Section 6: Security Training

6.1 Has the organization established a security training program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?



6.1.1 Documented policies and procedures for security awareness training (NIST SP 800-53: AT-1).



6.1.2 Documented policies and procedures for specialized training for users with significant information security responsibilities.



6.1.3 Security training content based on the organization and roles, as specified in organization policy or standards.



6.1.4 Identification and tracking of the status of security awareness training for all personnel (including employees, contractors, and other organization users) with access privileges that require security awareness training.



6.1.5 Identification and tracking of the status of specialized training for all personnel (including employees, contractors, and other organization users) with significant information security responsibilities that require specialized training.



6.1.6 Training material for security awareness training contains appropriate content for the organization (NIST SP 800-50,800-53).



Section 6: Security Training

6.2 Please provide any additional information on the effectiveness of the organization's Security Training Program that was not noted in the questions above.



Section 7: Plan Of Action & Milestones (POA&M)

7.1 Has the organization established a POA&M program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines and tracks and monitors known information security weaknesses? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?



7.1.1 Documented policies and procedures for managing IT security weaknesses discovered during security control assessments and that require remediation.



7.1.2 Tracks, prioritizes, and remediates weaknesses.



7.1.3 Ensures remediation plans are effective for correcting weaknesses.



7.1.4 Establishes and adheres to milestone remediation dates.



7.1.5 Ensures resources and ownership are provided for correcting weaknesses.



7.1.6 POA&Ms include security weaknesses discovered during assessments of security controls and that require remediation (do not need to include security weakness due to a risk-based decision to not implement a security control) (OMB M-04-25).



7.1.7 Costs associated with remediating weaknesses are identified (NIST SP 800-53, Rev. 3, Control PM-3 and OMB M-04-25).



Section 7: Plan Of Action & Milestones (POA&M)

7.1.8 Program officials report progress on remediation to CIO on a regular basis, at least quarterly, and the CIO centrally tracks, maintains, and independently reviews/validates the POA&M activities at least quarterly (NIST SP 800-53, Rev. 3, Control CA-5; OMB M-04-25).



7.2 Please provide any additional information on the effectiveness of the organization's POA&M Program that was not noted in the questions above.



Section 8: Remote Access Management

8.1 Has the organization established a remote access program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?



8.1.1 Documented policies and procedures for authorizing, monitoring, and controlling all methods of remote access (NIST 800-53: AC-1, AC-17).



8.1.2 Protects against unauthorized connections or subversion of authorized connections.



8.1.3 Users are uniquely identified and authenticated for all access (NIST SP 800-46, Section 4.2, Section 5.1).



8.1.4 Telecommuting policy is fully developed (NIST SP 800-46, Section 5.1).



8.1.5 If applicable, multi-factor authentication is required for remote access (NIST SP 800-46, Section 2.2, Section 3.3).



Section 8: Remote Access Management

8.1.6 Authentication mechanisms meet NIST SP 800-63 guidance on remote electronic authentication, including strength mechanisms.



8.1.7 Defines and implements encryption requirements for information transmitted across public networks.



8.1.8 Remote access sessions, in accordance with OMB M-07-16, are timed-out after 30 minutes of inactivity, after which re-authentication is required.



8.1.9 Lost or stolen devices are disabled and appropriately reported (NIST SP 800-46, Section 4.3, US-CERT Incident Reporting Guidelines).



8.1.10 Remote access rules of behavior are adequate in accordance with government policies (NIST SP 800-53, PL-4).



8.1.11 Remote access user agreements are adequate in accordance with government policies (NIST SP 800-46, Section 5.1, NIST SP 800-53, PS-6).



8.2 Please provide any additional information on the effectiveness of the organization's Remote Access Management that was not noted in the questions above.



8.3 Does the organization have a policy to detect and remove unauthorized (rogue) connections?



Section 9: Contingency Planning

9.1 Has the organization established an enterprise-wide business continuity/disaster recovery program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?



Section 9: Contingency Planning

- 9.1.1 Documented business continuity and disaster recovery policy providing the authority and guidance necessary to reduce the impact of a disruptive event or disaster (NIST SP 800-53: CP-1).
■
- 9.1.2 The organization has incorporated the results of its system's Business Impact Analysis (BIA) into the analysis and strategy development efforts for the organization's Continuity of Operations Plan (COOP), Business Continuity Plan (BCP), and Disaster Recovery Plan (DRP) (NIST SP 800-34).
■
- 9.1.3 Development and documentation of division, component, and IT infrastructure recovery strategies, plans and procedures (NIST SP 800-34).
■
- 9.1.4 Testing of system specific contingency plans.
■
- 9.1.5 The documented BCP and DRP are in place and can be implemented when necessary (FCD1, NIST SP 800-34).
■
- 9.1.6 Development of test, training, and exercise (TT&E) programs (FCD1, NIST SP 800-34, NIST SP 800-53).
■
- 9.1.7 Testing or exercising of BCP and DRP to determine effectiveness and to maintain current plans.
■
- 9.1.8 After-action report that addresses issues identified during contingency/disaster recovery exercises (FCD1, NIST SP 800-34).
■
- 9.1.9 Systems that have alternate processing sites (FCD1, NIST SP 800-34, NIST SP 800-53).
■
- 9.1.10 Alternate processing sites are not subject to the same risks as primary sites (FCD1, NIST SP 800-34, NIST SP 800-53).
■
- 9.1.11 Backups of information that are performed in a timely manner (FCD1, NIST SP 800-34, NIST SP 800-53).
■

Section 9: Contingency Planning

9.1.12 Contingency planning that considers supply chain threats.



9.2 Please provide any additional information on the effectiveness of the organization's Contingency Planning Program that was not noted in the questions above.



Section 10: Contractor Systems

10.1 Has the organization established a program to oversee systems operated on its behalf by contractors or other entities, including organization systems and services residing in the cloud external to the organization? Besides the improvement opportunities that may have been identified by the OIG, does the program includes the following attributes?



10.1.1 Documented policies and procedures for information security oversight of systems operated on the organization's behalf by contractors or other entities, including organization systems and services residing in a public cloud.



10.1.2 The organization obtains sufficient assurance that security controls of such systems and services are effectively implemented and comply with Federal and organization guidelines (NIST SP 800-53: CA-2).(Base)



10.1.3 A complete inventory of systems operated on the organization's behalf by contractors or other entities, including organization systems and services residing in a public cloud.



10.1.4 The inventory identifies interfaces between these systems and organization-operated systems (NIST SP 800-53: PM-5).



10.1.5 The organization requires appropriate agreements (e.g., MOUs, Interconnection Security Agreements, contracts, etc.) for interfaces between these systems and those that it owns and operates.



10.1.6 The inventory of contractor systems is updated at least annually.



Section 10: Contractor Systems

10.1.7 Systems that are owned or operated by contractors or entities, including organization systems and services residing in a public cloud, are compliant with FISMA requirements, OMB policy, and applicable NIST guidelines.



10.2 Please provide any additional information on the effectiveness of the organization's Contractor Systems Program that was not noted in the questions above.



Section 11: Security Capital Planning

11.1 Has the organization established a security capital planning and investment program for information security? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?



11.1.1 Documented policies and procedures to address information security in the capital planning and investment control (CPIC) process.



11.1.2 Includes information security requirements as part of the capital planning and investment process.



11.1.3 Establishes a discrete line item for information security in organizational programming and documentation (NIST SP 800-53: SA-2).



11.1.4 Employs a business case/Exhibit 300/Exhibit 53 to record the information security resources required (NIST SP 800-53: PM-3).



11.1.5 Ensures that information security resources are available for expenditure as planned.



11.2 Please provide any additional information on the effectiveness of the organization's Security Capital Planning Program that was not noted in the questions above.

