Office of Inspector General

FISMA Evaluation

# Evaluation of the Federal Labor Relations Authority Compliance with the Federal Information Security Management Act

## Fiscal Year 2014

## Report No. ER-15-01

## November 2014

Federal Labor Relations Authority
1400 K Street, N.W. Suite 250, Washington, D.C. 20424

## TABLE OF CONTENTS

## PURPOSE

Dembo, Jones, Healy, Pennington & Marshall, P.C. (Dembo Jones), on behalf of the Federal Labor Relations Authority (FLRA), Office of Inspector General (OIG), conducted an independent evaluation of the quality and compliance of the FLRA security program with applicable Federal computer security laws and regulations. Dembo Jones' evaluation focused on FLRA's information security required by the Federal Information Security Management Act (FISMA).

This report was prepared in conjunction with the Inspector General and Dembo Jones. The weaknesses discussed in this report should be included in FLRA's Fiscal Year (FY) 2014 report to the Office of Management and Budget (OMB) and Congress.

## BACKGROUND

On December 17, 2002, the President signed into law H.R. 2458, the E-Government Act of 2002 (Public Law 107-347). Title III of the E-Government Act of 2002, 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. This program includes providing security for information systems provided or managed by another agency, contractor, or other source. FISMA assigns specific responsibilities to agency heads and Inspectors General (IGs). It is supported by security policy promulgated through OMB, and risk-based standards and guidelines published in the National Institute of Standards and Technology (NIST) Special Publication (SP) series.

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. FISMA directs Federal agencies to report annually to the OMB Director, Comptroller General, and selected congressional committees on the adequacy and effectiveness of agency information security policies, procedures, and practices and compliance with FISMA. 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. Implementing adequate information security controls is essential to ensuring an organization can effectively meet its mission. The IG plays an essential role in supporting Federal agencies in identifying areas for improvement. In support of that critical goal the FLRA supports the development of a strategy to secure the FLRA computing environment which centers on providing confidentially, integrity, and availability.

## SCOPE AND METHODOLOGY

The scope of our testing focused on the FLRA network General Support System (GSS), however the testing also included the others systems in the FLRA system inventory. We conducted our testing through inquiry of FLRA personnel, observation of activities, inspection of relevant documentation, and the performance of technical security testing. Some examples of our inquiries with FLRA management and personnel included, but were not limited to, reviewing system security plans, access control, the risk assessments, and the configuration management processes.

## SUMMARY

During our FY 2014 evaluation, we noted that FLRA has taken great steps to improve the information security program. We also noted that FLRA does take information security weaknesses seriously. FLRA took action to remediate several weaknesses within specific control areas.

This year's FISMA testing resulted in two new findings. The first finding is that not all of the control objectives for the System Security Plans have been addressed as required by NIST 800-53 Revision 4. The second finding concerns the fact that audit plans have not been developed for the systems in our scope and security tools have not been deployed to investigate any possible suspicious activity and monitoring is not currently in operation. Our review included a follow up of all prior year deficiencies. There were a total of five prior issues, of which three are still open. Each of those issues has many elements that make up each finding. If any one of the elements is open, then that issue remains open.

## CURRENT YEAR FINDINGS

### *01 Continuous Monitoring / Security Plans*

**Condition:**
We reviewed the System Security Plans (SSPs) and Security Controls Assessments (SCAs) for all systems in scope and noted the following:

- Each of the SSPs have documentation to addresses the NIST 800-53 Revision 4 controls (e.g. account management, vulnerability scanning, and authenticator management), however, not all of the control objectives for each control are addressed.
- Due to the SSPs not containing the detail required in accordance with NIST 800-53 Revision 4, the controls were not assessed.

**Criteria:**
**NIST 800-53 Revision 4, PL-2 states:**
"Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions."

**NIST 800-53 Revision 4, CA-2 states:**
"Assesses the security controls in the information system and its environment of operation to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements."

**Cause:**
The cause is primarily because of a lack of personnel, budget, or time constraints to adequately document and/or assess all of the controls in NIST 800-53.

**Risk:**
Without appropriately documenting each of the control objectives, it will be unclear how specific controls are deployed. Without that clarity, controls may be deployed in a manner that is not commensurate with the risks of the system, which may expose the agency to vulnerabilities and exploitation attempts.

Without testing all of the controls, and on a continuous basis, there is a high likelihood that exploitation may occur as the controls are not deployed with the latest protective measures.

**Recommendation(s):**

1. Review all SSPs and ensure the documentation is clear and addresses each of the controls and all of their respective control objectives.
2. All controls within NIST 800-53 Revision 4 for the systems' categorization should be used as a starting point for determining the assessments and implementation of a continuous monitoring program. Then, management should determine which of those controls are critical. Those critical controls should be assessed every year. The remainder

of the controls should then be divided by three and then assessed over a three-year period, whereby 1/3 of the remaining controls are assessed each year. Ideally, the controls to be assessed each year should then be done on a quarterly basis by taking the annual set of controls and assessing ¼ each quarter. Upon completion of continuous monitoring, the agency should maintain metrics such as number of controls assessed on a monthly basis, number of deficiencies by family, etc.

**Management Response:**

The Agency took steps during the year to address the additional security requirements required by NIST 800-53 Revision 4. Management agrees with our finding and is developing a Plan of Action and Milestones (POA&M) that they are confident will effectively address the issues for which they have not accepted the risk.

**Condition:**
We interviewed key IT personnel and noted the following:

- Audit plans have not been developed or maintained for the systems in scope. Security tools have not been deployed for investigation of suspicious activities and monitoring is not currently in operation.

**Criteria:**
**NIST 800-53 Revision 4, AU-2 states:**
"Provides a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents."

**Cause:**
The cause is primarily because of a congressional hold on providing tapes to external contractors. The cause is also due to a lack of understanding because the congressional hold should not prevent the agency from protecting its data via the backup and storage at an off-site location.

**Risk:**
Without appropriately maintaining an audit plan which includes the deployment of audit tools for investigative purposes, FLRA runs the risk of not being able to identify the source of exploitation, thereby preventing future attacks on agency data.

**Recommendation(s):**

3. Develop and implement a formal audit plan. Also, deploy tools that will enable the agency to perform after the fact investigations of suspicious activities in the event that a breach has occurred.

**Management Response:**

Management agrees with our finding and is developing a POA&M to address our recommendation. The POA&M will include additional Management Responses and anticipated resolution dates.

## PRIOR YEAR FINDINGS

| # | Year Initiated | POA&M | Open / Closed |
|---|---|---|---|
| 1 | 2009 | **Develop a robust configuration management program in accordance with NIST Special Publication 800-53 Revision 3 Recommended Security Controls for Federal Information Systems.**<br><br>• The organization does not configure the information system to provide only essential capabilities and does not specifically prohibit and/or restrict the use of the following functions, ports, protocols, and/or services: [Assignment: organization-defined list of prohibited and/or restricted functions, ports, protocols, and/or services]. | Closed |
| 2 | 2009 | **Develop a robust contingency planning program in accordance with NIST Special Publication 800-53 Revision 3 Recommended Security Controls for Federal Information Systems.**<br><br>• The organization: (i) does not test and/or exercise the contingency plan for the information system [Assignment: organization-defined frequency, at least annually] using [Assignment: organization-defined tests and/or exercises] to determine the plan's effectiveness and the organization's readiness to execute the plan; and (ii) does not review the contingency plan test/exercise results and does not initiate corrective actions.<br><br>• The organization does not identify an alternate processing site and does not initiate necessary agreements to permit the resumption of information system operations for critical mission/business functions within [Assignment: organization-defined time period] when the primary processing capabilities are unavailable. | OPEN |
| 3 | 2009 | **Develop a robust system and communications protection program in accordance with NIST Special Publication 800-53 Revision 3 Recommended Security Controls for Federal Information Systems.**<br><br>• The information system does not protect against or limit the effects of the following types of denial of service attacks: [Assignment: organization-defined list of types of denial of service attacks or reference to source for current list]. | Closed |

| # | Year Initiated | POA&M | Open / Closed |
|---|---|---|---|
| | | • The information system doesn't protect the integrity of transmitted information.<br>• The information system doesn't protect the confidentiality of transmitted information. | |
| 4 | 2011 | **Dembo Jones obtained the latest Contingency Plan, as well as inquired about contingency testing in the event of a disaster. The following was noted:**<br>1. It was revealed that the latest Contingency Plan had not been signed or finalized.<br>2. Furthermore, there have been no formalized tests of a contingency to be prepared in the event of a disaster. | OPEN |
| 5 | 2011 | **It was revealed that the FLRA has not implemented the Homeland Security Presidential Directive (HSPD)-12 requirements across the agency.** | OPEN |

## APPENDIX A – MANAGEMENT RESPONSES

UNITED STATES OF AMERICA
**FEDERAL LABOR RELATIONS AUTHORITY**
1400 K STREET N.W. • WASHINGTON, D.C. 20424
(202) 218-7900 FAX: (202) 482-6778
www.FLRA.gov

November 10, 2014

**OFFICE OF THE CHAIRMAN**

Dana Rooney-Fisher
Inspector General
Federal Labor Relations Authority
1400 K Street NW
Washington, DC 20424

Dear Ms. Rooney-Fisher:

The FLRA extends its appreciation for the recently completed Federal Information Security Management Act (FISMA) evaluation of the FLRA information technology security program. The FLRA takes information security very seriously. The previous year's Inspector General audit reported five vulnerabilities ranging in severity from "Low to Moderate." I am pleased to report that we successfully mitigated two of the five vulnerabilities. And in 2014, there were additional security requirements required by NIST 800-53 Revision 4 and the requirement to implement Continuous Monitoring. The Agency took steps to address these requirements, as reflected in there only being two new findings that involve the additional security requirements. As a result, the FLRA's total number of open findings remains at five – three old and two new. The five vulnerabilities identified -- which continue to fall between "Low to Moderate" – involve the following issues:

- Contingency Plans and Testing
- Homeland Security Presidential Directive (HSPD) – 12
- Continuous monitoring
- NIST 800-53 Revision 4 (Update System Security Plan)

We are developing a Plan of Action and Milestones (POA&M) that we are confident will effectively address those remaining issues for which we have not, as explained during the evaluation process, accepted the risk. The POA&M will include Management Responses and anticipated resolution dates. We look forward to working with you on the resolution of the remaining issues over the course of Fiscal Year 2015.

Thank you for your continued support of this effort.

Respectfully,

Carol Waller Pope
Chairman

## APPENDIX B – OIG RESPONSES REPORTED IN CYBERSCOPE

# Inspector General

Section Report

2014

Annual FISMA Report

## Federal Labor Relations Authority

## 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?**

No

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

No

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

No

1.1.3 **Implemented ISCM for information technology assets.**

No

1.1.4 **Evaluate risk assessments used to develop their ISCM strategy.**

No

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

No

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).**

No

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).**

No

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.**

None

## Section 2: Configuration Management

## 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?**

Yes

*2.1.1* ***Documented policies and procedures for configuration management.***

Yes

2.1.2 **Defined standard baseline configurations.**

Yes

2.1.3 **Assessments of compliance with baseline configurations.**

Yes

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

Yes

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

Yes

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

Yes

2.1.7 **Process for timely and secure installation of software patches.**

Yes

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

Yes

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)**

Yes

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

Yes

## Section 2: Configuration Management

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.**

None

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

Yes

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

Yes

## 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?**

No

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

Yes

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

Yes

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

Yes

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).**

No

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).**

No

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).**

No

## Section 3: Identity and Access Management

3.1.7 **Ensures that the users are granted access based on needs and separation-of-duties principles.**

Yes

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).**

Yes

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.)**

N/A

3.1.10 **Ensures that accounts are terminated or deactivated once access is no longer required.**

Yes

3.1.11 **Identifies and controls use of shared accounts.**

N/A

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.**

None

## 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?**

No

4.1.1 **Documented policies and procedures for detecting, responding to, and reporting incidents (NIST SP 800-53: IR-1).**

Yes

4.1.2 **Comprehensive analysis, validation and documentation of incidents.**

No

## Section 4: Incident Response and Reporting

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).

Yes

4.1.4 When applicable, reports to law enforcement within established timeframes (NIST SP 800-61).

Yes

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).

No

4.1.6 Is capable of tracking and managing risks in a virtual/cloud environment, if applicable.

N/A

4.1.7 Is capable of correlating incidents.

Yes

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).

No

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.

None

## 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?

No

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

Yes

## Section 5: Risk Management

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.**

Yes

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.**

Yes

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.**

Yes

5.1.5 **Has an up-to-date system inventory.**

Yes

5.1.6 **Categorizes information systems in accordance with government policies.**

Yes

5.1.7 **Selects an appropriately tailored set of baseline security controls.**

Yes

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.**

No

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.**

No

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.**

Yes

## Section 5: Risk Management

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.**

No

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.**

Yes

5.1.13 **Senior officials are briefed on threat activity on a regular basis by appropriate personnel (e.g., CISO).**

Yes

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.**

Yes

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).**

Yes

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

Yes

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.**

None

## 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?**

Yes

## Section 6: Security Training

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

Yes

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

Yes

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

Yes

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.**

Yes

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.**

Yes

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

Yes

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.**

None

## 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?**

Yes

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

Yes

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

7.1.2 **Tracks, prioritizes, and remediates weaknesses.**

Yes

7.1.3 **Ensures remediation plans are effective for correcting weaknesses.**

Yes

7.1.4 **Establishes and adheres to milestone remediation dates.**

Yes

7.1.5 **Ensures resources and ownership are provided for correcting weaknesses.**

Yes

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).**

Yes

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

Yes

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).**

Yes

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.**

None

## 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?**

Yes

## Section 8: Remote Access Management

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

Yes

8.1.2 **Protects against unauthorized connections or subversion of authorized connections.**

Yes

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

Yes

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

Yes

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

Yes

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

Yes

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

Yes

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.**

Yes

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

Yes

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

Yes

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).**

Yes

## Section 8: Remote Access Management

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.

None

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

Yes

## 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?

No

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).

No

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).

No

9.1.3 Development and documentation of division, component, and IT infrastructure recovery strategies, plans and procedures (NIST SP 800-34).

No

9.1.4 Testing of system specific contingency plans.

No

9.1.5 The documented BCP and DRP are in place and can be implemented when necessary (FCD1, NIST SP 800-34).

No

9.1.6 Development of test, training, and exercise (TT&E) programs (FCD1, NIST SP 800-34, NIST SP 800-53).

No

## Section 9: Contingency Planning

9.1.7 Testing or exercising of BCP and DRP to determine effectiveness and to maintain current plans.

No

9.1.8 After-action report that addresses issues identified during contingency/disaster recovery exercises (FCD1, NIST SP 800-34).

No

9.1.9 Systems that have alternate processing sites (FCD1, NIST SP 800-34, NIST SP 800-53).

No

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).

No

9.1.11 Backups of information that are performed in a timely manner (FCD1, NIST SP 800-34, NIST SP 800-53).

Yes

9.1.12 Contingency planning that considers supply chain threats.

No

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.

None

## 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?

Yes

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.

Yes

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)

Yes

## Section 10: Contractor Systems

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.**

Yes

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

Yes

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.**

Yes

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

Yes

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.**

Yes

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.**

None

## 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?**

Yes

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

Yes

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

Yes

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

Yes

## Section 11: Security Capital Planning

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

Yes

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

Yes

**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.**

None

# CONTACTING THE OFFICE OF INSPECTOR GENERAL

IF YOU BELIEVE AN ACTIVITY IS WASTEFUL, FRAUDULENT, OR ABUSIVE OF FEDERAL FUNDS, CONTACT THE:

**HOTLINE (800)331-3572**

**HTTP://WWW.FLRA.GOV/OIG-HOTLINE**

EMAIL: OIGMAIL@FLRA.GOV
CALL: (202)218-7970 FAX: (202)343-1072
WRITE TO: 1400 K Street, N.W. Suite 250, Washington, D.C. 20424

The complainant may remain confidential; allow their name to be used; or anonymous. If the complainant chooses to remain anonymous, FLRA OIG cannot obtain additional information on the allegation, and also cannot inform the complainant as to what action FLRA OIG has taken on the complaint. Confidential status allows further communication between FLRA OIG and the complainant after the original complaint is received. The identity of complainants is protected under the provisions of the Whistleblower Protection Act of 1989 and the Inspector General Act of 1978. To learn more about the FLRA OIG, visit our Website at http://www.flra.gov/oig

Office of Inspector General

# FISMA Evaluation