Office of Inspector General

FISMA Evaluation

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

Fiscal Year 2012

Report No. ER-13-01

November 2012

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, 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) 2012 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 (the Federal Information Security Management Act), 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 Office of Management and Budget (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 Chief Information Officer is developing 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. We also utilized a software tool for identifying vulnerabilities on the network, as well as computers attached to the FLRA network.

SUMMARY

During our FY 2012 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. During the FY 2012 FISMA evaluation Dembo Jones performed a Vulnerability Assessment on the FLRA network, which included the servers, firewalls, and routers. This review also included testing 21 workstations that were connected to the FLRA network. Also included in the FISMA testing were controls from several families within the NIST 800-53 Rev. 3 publication.

This year's FISMA testing resulted in no new findings. This year's FISMA testing included a follow up of all prior year deficiencies. There were a total of twelve prior issues. 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.

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.** • 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]. – **OPEN**	OPEN
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.** • 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. – **OPEN – this was rolled up to a FY 2011 year finding.** • 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**	OPEN
3	2009	**Develop a robust incident response program in accordance with NIST Special Publication 800-53 Revision 3 Recommended Security Controls for Federal Information Systems.** • The organization does not train personnel in their incident response roles and responsibilities with respect to the information system and does not provide refresher training [Assignment: organization-defined frequency, at least annually]. - **OPEN – this was rolled up to a FY 2011 finding.**	OPEN

#	Year Initiated	POA&M	Open / Closed
4	2009	**Develop a robust planning program in accordance with NIST Special Publication 800-53 Revision 3 Recommended Security Controls for Federal Information Systems.** • The organization does not conduct a privacy impact assessment on the information system in accordance with OMB policy. – CLOSED.	Closed
5	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.** • 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]. – **OPEN** • The information system doesn't protect the integrity of transmitted information. - **OPEN** • The information system doesn't protect the confidentiality of transmitted information. - **OPEN**	OPEN
6	2011	**Dembo Jones performed a Vulnerability Assessment utilizing Nessus, which is a commercial software tool. This software deployed the latest plug-ins, which allowed for the scan to identify the latest vulnerabilities on both the network (servers, routers, firewalls, etc.) and a sample of desktops connected to the network. The results of this scan were as follows:** 1. The servers and workstations were not configured with the latest client application security patches. 2. Several hosts were running an outdated version of HP System Management Homepage. A web server was running an outdated version of Apache Tomcat 4.1.12. 3. The SYSDBA account of the Firebird server was configured with default credentials. 4. The host is running a clear text service (RSH).	Closed
7	2011	**Dembo Jones reviewed the audit settings for the server with Domain Controller access. This is the server responsible for managing authentication of FLRA users. It was revealed that Privileged Use is set to failure. Privileged Use is a setting within the audit events that tracks administrator users. Having this set to failure means if someone attempts to change something of a privileged nature, the audit log will only capture the failure of that event and not the success. If one of the privileged users changed something or created a user ID for adverse purposes, this would not be captured on the audit log for traceability and accountability purposes, as the change will have been completed successfully.**	Closed

#	Year Initiated	POA&M	Open / Closed
8	2011	**Dembo Jones obtained a listing of users with access to the Data Center. Upon this review, it was revealed that there were several personnel (four) who are not in Information Technology with access to the Data Center.**	Closed
9	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:** 1. It was revealed that the latest Contingency Plan had not been signed or finalized. 2. Furthermore, there have been no formalized tests of a contingency to be prepared in the event of a disaster.	OPEN
10	2011	**Dembo Jones inquired about incident response with IT personnel. It was revealed that there is no Incident Response training for IT personnel.**	OPEN
11	2011	**It was revealed that the FLRA has not implemented the Homeland Security Presidential Directive (HSPD)-12 requirements across the agency.**	OPEN
12	2011	**Privacy Threshold Assessments (PTA) need to be performed for those systems without PTAs. The PTA is a process to identify any and all Personally Identifiable Information (PII) elements. If any of those elements (alone or in combination) can be traced to an individual, the PII is then considered Information in Identifiable Form (IIF). PIAs are required for systems that have IIF. Further, once the Privacy Impact Assessment (PIA) is completed, the IIF should be categorized as either low, moderate, or high.**	Closed

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 14, 2012

OFFICE OF THE CHAIRMAN

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

Dear Ms. Rooney-Fischer:

The FLRA extends its appreciation for the recently completed Federal Information Security Management Act (FISMA) evaluation of the FLRA information technology systems security. The FLRA takes information security very seriously. The previous year's Inspector General audit reported twelve vulnerabilities ranging in severity from "Low to Moderate." I am pleased to report that we successfully mitigated five of those twelve vulnerabilities. This is a significant accomplishment given that just two years ago the agency had twenty vulnerabilities -- some of which were identified as "High." Currently, the seven vulnerabilities identified -- which continue to fall between "Low to Moderate" -- involve the following issues:

- Audit settings
- Contingency Plans and Testing
- Incident Response Training
- Awareness Training
- Homeland Security Presidential Directive (HSPD) – 12

We are developing a Plan of Action and Milestones (POA&M) that we are confident will effectively address each of the remaining issues. 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 2012.

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

2012

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:**

Yes

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

Yes

1.1.2 **Documented strategy and plans for continuous monitoring (NIST 800-37 Rev 1, Appendix G)**

Yes

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

Yes

1.1.4 **Provides authorizing officials and other key system officials with security status reports covering updates to security plans and security assessment reports, as well as POA&M additions and updates with the frequency defined in the strategy and/or plans (NIST 800-53, NIST 800-53A)**

Yes

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**

N/A

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 **Standard baseline configurations defined**

Yes

For Official Use Only

Section 2: Configuration Management

2.1.3 **Assessing for 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, FDCC/USGCB secure configuration settings fully implemented and any deviations from FDCC/USGCB baseline settings fully documented**

No

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 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 800-53: CM-4, CM-6, RA-5, SI-2)**

No

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

Yes

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.**

N/A

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:**

Yes

For Official Use Only

Section 3: Identity and Access Management

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

Yes

3.1.2 **Identifies all users, including federal employees, contractors, and others who access Organization systems (NIST 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 800-53, IA-2)**

No

3.1.5 **Organization has adequately 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 **Ensures that the users are granted access based on needs and separation of duties principles**

Yes

3.1.7 **Identifies devices with IP addresses that are attached to the network and distinguishes these devices from users (For example: IP phones, faxes, printers are examples of devices attached to the network that are distinguishable from desktops, laptops or servers that have user accounts)**

Yes

3.1.8 **Identifies all User and Non-User Accounts (refers to user accounts that are on a system. Examples of non-user accounts are accounts such as an IP that is set up for printing. Data user accounts are created to pull generic information from a database or a guest/anonymous account for generic login purposes that are not associated with a single user or a specific group of users)**

Yes

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

Yes

3.1.10 **Identifies and controls use of shared accounts**

Yes

For Official Use Only

Section 3: Identity and Access Management

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.**

N/A

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 800-53: IR-1)**

No

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

No

4.1.3 **When applicable, reports to US-CERT within established timeframes (NIST 800-53, 800-61, and OMB M-07-16, M-06-19)**

No

4.1.4 **When applicable, reports to law enforcement within established timeframes (SP 800-86)**

No

4.1.5 **Responds to and resolves incidents in a timely manner, as specified in Organization policy or standards, to minimize further damage. (NIST 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**

No

4.1.7 **Is capable of correlating incidents**

No

4.1.8 **There is sufficient incident monitoring and detection coverage in accordance with government policies (NIST 800-53, 800-61, and OMB M-07-16, M-06-19)**

No

For Official Use Only

Section 4: Incident Response and Reporting

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.**

N/A

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:**

Yes

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

Yes

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 800-37, Rev.1**

Yes

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

Yes

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

Yes

5.1.5 **Categorizes information systems in accordance with government policies**

Yes

5.1.6 **Selects an appropriately tailored set of baseline security controls**

Yes

5.1.7 **Implements the tailored set of baseline security controls and describes how the controls are employed within the information system and its environment of operation**

Yes

For Official Use Only

Section 5: Risk Management

5.1.8 **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**

Yes

5.1.9 **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

5.1.10 **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**

Yes

5.1.11 **Information system specific risks (tactical), mission/business specific risks and organizational level (strategic) risks are communicated to appropriate levels of the organization.**

Yes

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

Yes

5.1.13 **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

5.1.14 **Security authorization package contains system security plan, security assessment report, and POA&M in accordance with government policies. (SP 800-18, SP 800-37)**

Yes

5.1.15 **Security authorization package contains Accreditation boundaries for Organization information systems defined in accordance with government policies.**

Yes

For Official Use Only

Section 5: Risk Management

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.

N/A

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

6.1.1 Documented policies and procedures for security awareness training (NIST 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 (SP 800-50, SP 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.

N/A

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

For Official Use Only

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 requiring remediation**

Yes

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 are provided for correcting weaknesses**

Yes

7.1.6 **POA&Ms include security weaknesses discovered during assessments of security controls and requiring 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 and contractors 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, and 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.**

N/A

Section 8: Remote Access Management

For Official Use Only

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

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 800-46, Section 4.2, Section 5.1)

Yes

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

Yes

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

Yes

8.1.6 Authentication mechanisms meet NIST Special Publication 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 to OMB M-07-16, are timed-out after 30 minutes of inactivity after which re-authentication are required

Yes

8.1.9 Lost or stolen devices are disabled and appropriately reported (NIST 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 800-53, PL-4)

Yes

For Official Use Only

Section 8: Remote Access Management

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

Yes

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.

N/A

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 800-53: CP-1)

Yes

9.1.2 The Organization has performed an overall Business Impact Analysis (BIA) (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)

Yes

9.1.4 Testing of system specific contingency plans

No

9.1.5 The documented business continuity and disaster recovery plans are in place and can be implemented when necessary (FCD1, NIST SP 800-34)

Yes

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

No

For Official Use Only

Section 9: Contingency Planning

9.1.7 **Performance of regular ongoing testing or exercising of business continuity/disaster recovery plans 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 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 consider supply chain threats**

N/A

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.**

N/A

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 public cloud**

Yes

For Official Use Only

Section 10: Contractor Systems

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

Yes

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 public cloud

Yes

10.1.4 The inventory identifies interfaces between these systems and Organization-operated systems (NIST 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 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.

N/A

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

For Official Use Only

Section 11: Security Capital Planning

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 800-53: SA-2)**

Yes

11.1.4 **Employs a business case/Exhibit 300/Exhibit 53 to record the information security resources required (NIST 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.**

N/A

For Official Use Only

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