



Office of Inspector General

FISMA Evaluation

**EVALUATION OF THE
FEDERAL LABOR RELATIONS
AUTHORITY COMPLIANCE
WITH THE FEDERAL
INFORMATION SECURITY
MANAGEMENT ACT**

Fiscal Year 2015

Report No. ER-16-01

November 2015

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

TABLE OF CONTENTS

PURPOSE.....2
BACKGROUND2
SCOPE AND METHODOLOGY3
SUMMARY.....3
CURRENT YEAR FINDINGS4
 01 Timely Remediation of Vulnerabilities.....4
 02 Personnel Termination5
 03 Incident Response Plan, Testing, and Training.....6
 04 Access Authorization Management7
PRIOR YEAR FINDINGS9
APPENDIX A – MANAGEMENT RESPONSES11
APPENDIX B – OIG RESPONSES REPORTED IN CYBERSCOPE.....14

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) 2015 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 confidentiality, 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 2015 evaluation, we noted that FLRA has taken 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.

There, however, are four new deficiencies that we identified. This year's FISMA testing included a follow up of all prior year deficiencies. There were a total of five prior issues, of which three are still open.

CURRENT YEAR FINDINGS

01 Timely Remediation of Vulnerabilities

Condition:

Scan results were reviewed over a two week period to assess the timely remediation of any Medium and High vulnerabilities. Upon review of those scan results, we were unable to discern a total list of Low, Medium, and High risks, as well as how long it took to remediate those deficiencies. As a result, the condition is that deficiencies are not remediated in a timely manner.

Criteria:**NIST 800-53, Revision 4, RA-5 states:**

“Remediates legitimate vulnerabilities in accordance with an organizational assessment of risk.”

Cause:

The cause is primarily because of a lack of personnel, budget, and time constraints to adequately document and/or assess all of the controls in NIST 800-53, Revision 4. Documentation of the procedures performed in this area is lacking.

Risk:

By having vulnerabilities exposed to the agency, there is the risk that adversaries can take advantage of those weaknesses and gain access to FLRA’s data, which ultimately may lead to a lack of integrity and/or confidentiality for the agency.

Recommendation(s):

1. All vulnerabilities should be reviewed in terms of their risk classification (e.g. High, Medium, and Low). High vulnerabilities should be remediated within 1 business day and Medium vulnerabilities should be remediated within 3-5 business days. Documentation in these areas needs to be improved.

Management Response:

Management noted that vulnerabilities were remediated in accordance with the guidelines, but documentation of the remediation was lacking. They intend to implement a more stringent documentation policy of all steps to remediate vulnerabilities in a timely fashion.

02 Personnel Termination

Condition:

Upon review of the users that were terminated from the agency, it was not discernable how many days it took to remove the users' access after their respective termination date.

Criteria:

NIST 800-53, Revision 4, PS-4 states:

"The organization, upon termination of individual employment:

- a. Disables information system access within an organization-defined time period."

Cause:

The CIO indicated that they do remove the access from users on the day of termination, however, documentation of this is lacking.

Risk:

If an agency has terminated users without having disabled their access in a timely manner, there is the risk that those user's IDs can be used for exploitation and adversarial actions against the agency.

Recommendation(s):

2. Any user that is terminated from the agency should have their access disabled within 5 business days. This needs to be documented to provide evidence that this is being done.

Management Response:

Management noted that upon termination, the FLRA takes many steps to ensure account access and Agency owned assets are dealt with appropriately. The FLRA will update its policy and documentation showing the actions taken.

03 Incident Response Plan, Testing, and Training

Condition:

Upon review of Incident Response planning and testing; the following was noted:

- There is no testing of the current Incident Response environment.
- There is also no training provided to the IT staff with respect to preparing for and managing incidents.

Criteria:

NIST 800-53, Revision 4, IR-2 states:

“The organization provides incident response training to information system users consistent with assigned roles and responsibilities:

- a. Within 30 days of assuming an incident response role or responsibility;
- b. b. When required by information system changes; and
- c. Annually.”

Cause:

The cause is primarily because of a lack of personnel, budget, and time constraints. We understand that plans are currently being formulated to conduct the required planning, testing and training.

Risk:

Without a finalized Incident Response Plan, there is the risk that when an incident occurs, the remediation of such an incident will not be performed in a manner that was approved by the Office of Information Technology (OIT). This may lead to an untimely remediation of the incident thereby affecting agency data and systems. Without testing of the Incident Response environment, there is the risk that the OIT and other staff members will be unprepared for when an incident actually does occur.

Recommendation(s):

3. Incident Response prevention, detection and correction should be tested on an annual basis.

Management Response:

Management responded that the FLRA will finalize its Incident Response Plan and all IT personnel will participate in all aspects of Incident Response planning, testing, and training as coordinated by the FLRA’s Information Systems Security Manager.

04 Access Authorization Management

Condition:

Upon review of a sample of a set of users for assessing their access authorizations; the following was noted:

- Access authorization forms (paper or electronic) are not being maintained to ensure that users' rights are commensurate with what was approved.
- An annual recertification of users' access rights are not being performed.

Criteria:

NIST 800-53, Revision 4, IA-4 states:

“The organization manages information system identifiers by:

a. Receiving authorization from organization-defined personnel or roles to assign an individual, group, role, or device identifier;”

“The organization requires that the registration process to receive an individual identifier includes supervisor authorization.”

NIST 800-53, Revision 4, AC-2 states:

“Specifies authorized users of the information system; group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;”

“Requires approvals by organization-defined personnel or roles for requests to create information system accounts;”

“Authorizes access to the information system based on:

1. A valid access authorization;
2. Intended system usage; and
3. Other attributes as required by the organization or associated missions/business functions;”

“Reviews accounts for compliance with account management requirements organization-defined frequency”.

Cause:

The cause is primarily because of a lack of personnel, budget, and time constraints to adequately document and/or assess all of the controls in NIST 800-53, Revision 4.

Risk:

Without maintaining and reviewing users' access rights on an annual basis, there is the risk that users will be authorized in excess of what they were approved for, thereby creating an environment where a user can potentially exploit FLRA's systems and data.

Recommendation(s):

4. All users' access rights upon initiation should have their access rights reviewed, approved, and subsequently maintained for audit purposes.
5. On an annual basis, all FLRA employees should have their access reviewed to ensure it is still commensurate with their job functions. Consider having supervisors across the FLRA assist in this review of employees in their departments and provide the OIT with the analysis.

Management Response:

Management believes the FLRA did perform the necessary audits and permission confirmation practices, however, the processes were not properly documented. The Information Systems Security Manager will document the appropriate steps for these activities in a verifiable manner.

PRIOR YEAR FINDINGS

#	Year Initiated	POA&M	Open / Closed
1	2009	<p><i>Develop a robust contingency planning program in accordance with NIST Special Publication 800-53 Revision 3 Recommended Security Controls for Federal Information Systems.</i></p> <ul style="list-style-type: none"> • 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. • 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
2	2011	<p><i>Dembo Jones obtained the latest Contingency Plan, as well as inquired about contingency testing in the event of a disaster. The following was noted:</i></p> <ul style="list-style-type: none"> • It was revealed that the latest Contingency Plan had not been signed or finalized. • Furthermore, there have been no formalized tests of a contingency to be prepared in the event of a disaster. 	OPEN
3	2011	<p><i>It was revealed that the FLRA has not implemented the Homeland Security Presidential Directive (HSPD)-12 requirements across the agency.</i></p> <p>FY 2015 status: The CIO implemented a waiver for mobile computers, until an acceptable solution could be attained to rapidly respond to lost PIV Cards.</p>	CLOSED
4	2014	<p><i>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. Furthermore, because there was no continuous monitoring in terms of periodic testing, POA&Ms were not completed timely or not completed at all.</i></p>	OPEN

#	Year Initiated	POA&M	Open / Closed
		<ul style="list-style-type: none"> • Review all SSPs and ensure the documentation is clear and addresses each of the controls and all of their respective control objectives. • 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 1/4 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. • Ensure any deficiencies as a result of the continuous monitoring assessments will be clearly and timely reported as a POA&M. 	
5	2014	<p><i>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.</i></p> <ul style="list-style-type: none"> • 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. <p>FY 2015 status: Our recommendations were implemented during FY 2015.</p>	CLOSED

APPENDIX A – MANAGEMENT RESPONSES




UNITED STATES OF AMERICA
FEDERAL LABOR RELATIONS AUTHORITY
1400 K STREET N.W. • WASHINGTON, D.C. 20424
www.FLRA.gov

November 6, 2015

MEMORANDUM

TO: Dana Rooney-Fisher
Inspector General

FROM: Sarah Whittle ~~Spooner~~ 
Executive Director

SUBJECT: Follow-up Response and Action Plan Regarding Compliance with the Federal Information Security Management Act (FISMA) Fiscal Year (FY) 2015 Report

Thank you for the opportunity to provide a follow-up memo addressing the FISMA FY15 Report. Please find attached the Plan of Action and Milestones (POAM) that was developed in response to the Report. Plans have been developed for mitigating the vulnerabilities and are expected to be corrected by September 2016.

We look forward to continuing to work with you on addressing and resolving any outstanding matters.

#	Finding	Management Response	Corrective Timeline
1	<p>Develop a robust contingency planning program in accordance with NIST Special Publication 800-53 Revision 3 Recommended Security Controls for Federal Information Systems .</p> <p>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</p> <p>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.</p>	<p>Updating Draft COOP plan to include an information technology continuity of operations plan (COOP), as well as a engineer a series of exercises to test the COOP. Work with Administrative Services Group to finalize the FLRA COOP plan.</p> <p>IRMD is currently architecting a solution that will establish a cold alternate processing site at the FLRA Chicago regional office. While this effort has significant technical and economic barriers to completion, IRMD is confident the site can be established.</p> <p>Update: IRMD received the replacement server equipment and has begun staging it to replace the old equipment. The plan is to use the old equipment for the new COOP offsite.</p>	Spring 2016
2	<p>Dembo Jones obtained the latest Contingency Plan, as well as inquired about contingency testing in the event of a disaster. The following was noted:</p> <p>1. It was revealed that the latest Contingency Plan had not been signed or finalized.</p>	<p>See finding #2 - FLRA is establishing a COOP site and updating the draft COOP plan.</p>	Spring 2016
3	<p>It was revealed that the FLRA has not implemented the Homeland Security Presidential Directive (HSPD)-12 requirements across the agency.</p> <p>FY 2015 status: The CIO requested a waiver from OMB for mobile computers. The waiver was granted</p>	<p>While FLRA implemented mandatory physical HSPD-12 access, mandatory logical login presents risk that could cause mobile users undue burden where they could lose access for days or even weeks, depending on when and where they can get back into the office. The FLRA has decided to issue a waiver for all mobile workstations until a faster more appropriate solution can be developed. With this waiver, the FLRA will meet the HSPD-12 mandatory logical login requirement. The Agency waiver was completed Feb. 2015.</p>	Closed
4	<p>Continuous Monitoring / Security Plans</p> <p>Dembo Jones reviewed the System Security Plans (SSPs) and Security Controls Assessments (SCAs) for all systems in scope and noted the following:</p> <p>1 - 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.</p> <p>2 - Due to the SSPs not containing the detail required in accordance with NIST 800-53 Revision 4, the controls were not assessed.</p>	<p>FLRA took steps during the year to address the additional security requirements required by NIST 800-53 Revision 4. We understand our System Security Plan needs to be updated, in order to fully implement continuous monitoring. FLRA's current System Security Plan is much more of a narrative, which was much more common in years past. As such, the document does not specifically address each control as required by OMB. This will be addressed in the coming year as part of the security documentation refresh. All the critical security controls will be addressed, and a schedule will be created to adequately address the remaining controls in a rotating cycle once every three years.</p>	Spring 2016
5	<p>Auditing</p> <p>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.</p> <p>FY 2015 status: Our recommendations were implemented during FY 2015.</p>	<p>The FLRA deployed several continuous monitoring products and implemented software to serve as a central control point that will allow for the investigation of compromises. In addition, the FLRA implemented new backup technologies that greatly improve the agencies backup and recovery resources in a geographically diverse manner.</p>	Closed

6	<p>Timely Remediation of Vulnerabilities</p> <p>Scan results were reviewed over a two week period to assess the timely remediation of any Medium and High vulnerabilities. Upon review of those scan results, we were unable to discern a total list of Low, Medium, and High risks, as well as how long it took to remediate those deficiencies. As a result, the condition is that deficiencies are not remediated in a timely manner.</p>	<p>The FLRA takes the remediation of vulnerabilities seriously and has committed to NIST 800-53, Revision 4, RA-5. While vulnerabilities were remediated in accordance with this guideline, as noted by the auditor, the documentation of said remediation was lacking. The FLRA intends to implement a more stringent documentation policy of all steps taken to remediate vulnerabilities in a timely manner.</p>	Spring 2016
7	<p>Personnel Termination</p> <p>Upon review of the users that were terminated from the agency, it was not discernable how many days it took to remove the users' access after their respective termination date.</p>	<p>Upon termination, the FLRA takes many steps to ensure account access and Agency owned assets are dealt with appropriately. The FLRA will update its policy and documentation showing the actions taken.</p>	Spring 2016
8	<p>Upon review of Incident Response planning and testing, the following was noted:</p> <p>There is no testing of the current incidence response environmentg</p> <p>There is no training provided to the IT staff with respect to preparing for and managing incidents</p>	<p>The FLRA will finalize its Incident Response Plan and all IT personnel will participate in all aspects of Incident Response planning, testing, and training as coordinated by the FLRA's Information Systems Security Manager.</p>	September 2016
9	<p>Access Authorization</p> <p>Upon review of a sample of a set of users for assessing their access authorizations, the following was noted:</p> <p>Access authorization forms (paper or electronic) are not being maintained to ensure that users' rights are commensurate with what was approved</p> <p>An annual recertification of users' access rights are not being performed.</p>	<p>While the FLRA did perform the necessary audits and permission confirmation practices, the processes were not properly documented. This made it difficult for the auditor to confirm. As with the above findings, the Information Systems Security Manager will document the appropriate steps for these activities in a verifiable manner.</p>	Spring 2016

APPENDIX B – OIG RESPONSES REPORTED IN CYBERSCOPE

For Official Use Only

Inspector General

Section Report

2015
Annual FISMA
Report

Federal Labor Relations Authority

For Official Use Only

Section 1: Continuous Monitoring Management

- 1.1 Utilizing the ISCM maturity model definitions, please assess the maturity of the organization's ISCM program along the domains of people, processes, and technology. Provide a maturity level for each of these domains as well as for the ISCM program overall.
- 1.1.1 Please provide the D/A ISCM maturity level for the People domain.
Managed & Measurable (Level 4)
 - 1.1.2 Please provide the D/A ISCM maturity level for the Processes domain.
Consistently Implemented (Level 3)
 - 1.1.3 Please provide the D/A ISCM maturity level for the Technology domain
Defined (Level 2)
 - 1.1.4 Please provide the D/A ISCM maturity level for the ISCM Program Overall.
Defined (Level 2)
- 1.2 Please provide any additional information on the effectiveness of the organization's Information Security Continuous Monitoring Management Program that was not noted in the maturity model above.
None

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?
- 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

Section 2: Configuration Management

- 2.1.4 Process for timely (as specified in organization policy or standards) remediation of scan result findings.
Yes
- 2.1.5 For Windows-based components, USGCB secure configuration settings are fully implemented (when available), and any deviations from USGCB baseline settings are fully documented.
Yes
- 2.1.6 Documented proposed or actual changes to hardware and software baseline configurations.
Yes
- 2.1.7 Implemented software assessing (scanning) capabilities (NIST SP 800-53: RA-5, SI-2).
Yes
- 2.1.8 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).
No
- 2.1.9 Patch management process is fully developed, as specified in organization policy or standards, including timely and secure installation of software patches (NIST SP 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.
Yes
- 2.3 Does the organization have an enterprise deviation handling process and is it integrated with an automated scanning capability?
Yes
- 2.3.1 Is there a process for mitigating the risk introduced by those deviations? A deviation is an authorized departure from an approved configuration. As such it is not remediated but may require compensating controls to be implemented.
Yes

Section 3: Identity and Access Management

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 which 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 (HSPD 12, NIST SP 800-53, AC-2).
Yes
- 3.1.3 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
- 3.1.4 Organization has 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).
Yes
- 3.1.5 Ensures that the users are granted access based on needs and separation-of-duties principles.
No
- 3.1.6 Distinguishes hardware assets that have user accounts (e.g., desktops, laptops, servers) from those without user accounts (e.g. IP phones, faxes, printers).
Yes
- 3.1.7 Ensures that accounts are terminated or deactivated once access is no longer required according to organizational policy.
No
- 3.1.8 Identifies and controls use of shared accounts.
Yes

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.
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).

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 SP 800-53, 800-61; OMB M-07-16, M-06-19).

No

4.1.4 When applicable, reports to law enforcement and the agency Inspector General within established timeframes.

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 SP 800-53, 800-61; OMB M-07-16, M-06-19).

No

4.1.6 Is capable of correlating incidents.

No

4.1.7 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

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.
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 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.
No
 - 5.1.2 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.
No
 - 5.1.3 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.
No
 - 5.1.4 Has an up-to-date system inventory.
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 and describes how the controls are employed within the information system and its environment of operation.
Yes
 - 5.1.7 Implements the approved set of tailored baseline security controls specified in metric 5.1.6.
No

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.
No
- 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.
No
- 5.1.10 Information-system-specific risks (tactical), mission/business-specific risks, and organizational-level (strategic) risks are communicated to appropriate levels of the organization.
No
- 5.1.11 Senior officials are briefed on threat activity on a regular basis by appropriate personnel (e.g., CISO).
No
- 5.1.12 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.
No
- 5.1.13 Security authorization package contains system security plan, security assessment report, POA&M, accreditation boundaries in accordance with government policies for organization information systems (NIST SP 800-18, 800-37).
No
- 5.1.14 The organization has an accurate and complete inventory of their cloud systems, including identification of FedRAMP approval status.
Yes
- 5.1.15 For cloud systems, the organization can identify the security controls, procedures, policies, contracts, and service level agreements (SLA) in place to track the performance of the Cloud Service Provider (CSP) and manage the risks of Federal program and personal data stored on cloud systems.
Yes

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.
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

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)

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
- 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 and provides adequate justification for missed 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 in terms of dollars (NIST SP 800-53: PM-3; 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: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

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 SP 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 Authentication mechanisms meet NIST SP 800-63 guidance on remote electronic authentication, including strength mechanisms.
Yes
- 8.1.6 Defines and implements encryption requirements for information transmitted across public networks.
Yes
- 8.1.7 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
- 8.1.8 Lost or stolen devices are disabled and appropriately reported (NIST SP 800-46, Section 4.3; US-CERT Incident Reporting Guidelines).
Yes
- 8.1.9 Remote access rules of behavior are adequate in accordance with government policies (NIST SP 800-53, PL-4).
Yes

Section 8: Remote Access Management

- 8.1.10 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
- 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?
No

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 and Business Process Analysis into the appropriate analysis and strategy development efforts for the organization's Continuity of Operations Plan, Business Continuity Plan, and Disaster Recovery Plan (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

Section 9: Contingency Planning

- 9.1.5 The documented BCP and DRP are in place and can be implemented when necessary (FCDI, NIST SP 800-34).
No
- 9.1.6 Development of test, training, and exercise (TT&E) programs (FCDI, NIST SP 800-34, NIST SP 800-53).
No
- 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 (FCDI, NIST SP 800-34).
No
- 9.1.9 Alternate processing sites are not subject to the same risks as primary sites. Organization contingency planning program identifies alternate processing sites for systems that require them (FCDI, NIST SP 800-34, NIST SP 800-53).
No
- 9.1.10 Backups of information that are performed in a timely manner (FCDI, NIST SP 800-34, NIST SP 800-53).
Yes
- 9.1.11 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 for organization systems and services residing in a cloud external to the organization? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?
Yes

Section 10: Contractor Systems

- 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 other government agencies), including organization systems and services residing in a public, hybrid, or private cloud.
Yes
- 10.1.2 The organization obtains sufficient assurance that security controls of such systems and services are effectively implemented and compliant with FISMA requirements, OMB policy, and applicable NIST guidelines (NIST SP 800-53: CA-2).
Yes
- 10.1.3 A complete inventory of systems operated on the organization's behalf by contractors or other entities, (including other government agencies), including organization systems and services residing in public, hybrid, or private 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
- 10.2 Please provide any additional information on the effectiveness of the organization's Contractor Systems Program that was not noted in the questions above.
None

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](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