Office of Inspector General

FISMA Evaluation

Evaluation of the Federal Labor Relations Authority's Compliance with the Federal Information Security Management Act of 2014 for

Fiscal Year 2018

Report No. MAR-19-01

October 2018

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

CONTENTS

Evaluation Report

Appendices

Abbreviations

Dembo Jones	Dembo Jones, P.C.
FISMA	Federal Information Security Modernization Act
FLRA	Federal Labor Relations Authority
FY	Fiscal Year
IG	Inspector General
IT	Information Technology
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget

Evaluation of FLRA’s Compliance with the FISMA FY 2018

Report No. MAR-19-01 ***October 29, 2018***

The Honorable Colleen Duffy Kiko
Chairman

Dembo Jones, 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 Modernization Act (FISMA). The weaknesses discussed in this report should be included in FLRA’s Fiscal Year (FY) 2018 report to the Office of Management and Budget (OMB) and Congress.

Results in Brief

During our FY 2018 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.

This year’s FISMA testing included a follow up of all prior year recommendations. There was a total of 1 prior recommendation, which has been closed. There were several new findings as follows:

- Timely deployment of patches;
- Rules of behavior lacking the latest guidance in accordance with National Institute of Standards and Technology (NIST);
- Lack of disabling users after 180 days of inactivity; and
- Lack of audit log reviews.

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 NIST Special Publication 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, 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.

Dembo Jones, P.C.

Dembo Jones, P.C.

Rockville, Maryland
October 29, 2018

Appendix 1
Current Year Findings and Recommendations

1. Timely Deployment of Patches

The agency's Office of Chief Information Officer is responsible for performing scans of the agency's information systems to identify and remediate vulnerabilities. Vulnerability scanning includes, for example: (i) scanning for missing and/or out of date patches; (ii) scanning for functions, ports, protocols, and services that should not be accessible to users or devices; and (iii) scanning for improperly configured or incorrectly operating information flow control mechanisms. Remediation is the correction of vulnerability or eliminating a threat.

Condition:

There have been several false positives with regard to ensuring that patch management is complete and accurate. As a result, although scanning is conducted monthly, there are a large number of patches that appear to be out of date with the potential that some of them are false positives.

Criteria:

NIST 800-53, Revision 4, Risk Assessment (RA)-5 states:

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

Cause:

Due to a lack of patch management software applications, FLRA did not adequately address patching.

Effect:

By having patches that are not up to date, 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:

1. Purchase and deploy a patch management software application to ensure that patches are managed and deployed in a timely manner.

Management Response:

Management agrees with our recommendation.

2. Rules of Behavior Lacking the Latest Guidance in Accordance with NIST

Condition:

Upon review of a sampled set of users for their evidence of accepting the Rules of Behavior, the following was noted:

- The Rules of Behavior that is required for all employees and contractors didn't include the provisions for social media, networking sites, posting information on commercial websites, and sharing of information.

Criteria:

NIST 800-53, Revision 4, Planning (PL)-4 states:
"The organization includes in the rules of behavior, explicit restrictions on the use of social media and networking sites, posting information on commercial websites, and sharing information system account information."

Cause:

Due to a lack of personnel, budget, or time constraints, FLRA did not adequately include all provisions within their Rules of Behavior training in accordance with NIST 800-53, Revision 4.

Effect:

Without ensuring that the Rules of Behavior includes stipulations for social media, posting on networking sites, and sharing of information; there is the increased risk that employees and contractors will be unaware of their roles and responsibilities. Without knowledge of their roles and responsibilities, it further increases the risk that the agency will be exposed to unforeseen risks through the sharing, posting or dissemination of data which can be used for subsequent exploitation.

Recommendations:

2. Revise the Rules of Behavior to include social media, networking sites, posting on commercial websites and sharing of data.
3. Ensure all employees and contractors sign the revised Rules of Behavior as evidence of their acceptance.

Management Response:

Management agrees with our recommendations.

3. Lack of Disabling Users after 180 days of Inactivity

Condition:

Dembo Jones reviewed various password complexity settings on servers supporting the FLRA applications and noted the following:

- Users are not disabled after a period of 180 days of inactivity.

Criteria:

NIST 800-53, Revision 4, Access Controls (AC)-2, states: "Creating, enabling, modifying, disabling, and removing accounts (including adding and deleting members from groups or roles)."

Cause:

Due to a lack of personnel, budget, or time constraints, FLRA did not adequately review and implement appropriate disabling of user accounts.

Effect:

Without appropriate password complexity settings (especially for Information Technology (IT) related personnel), users will have authentication credentials that are weak and susceptible to exploitation. Weak authentication for the IT personnel will raise the risk of spoofing a user (pretending to be someone else) and access gained can be used for adverse actions.

Recommendation:

4. Ensure that users are automatically disabled after a period of 180 days of inactivity.

Management Response:

Management agrees with our recommendation.

4. Lack of Audit Log Reviews

Condition:

Dembo Jones reviewed the audit log settings and it was determined that although there was sufficient space to house the logs, the audit logs were not being timely reviewed.

Criteria:

NIST 800-53, Revision 4, Audit and Accountability (AU)-6, states: "The organization:

a. Reviews and analyzes information system audit records [Assignment: organization-defined frequency] for indications of inappropriate or unusual activity;

b. Reports findings to [Assignment: organization-defined personnel];

c. Adjusts the level of audit review, analysis, and reporting within the information system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information; and

d. Specifies the permitted actions for each [Selection (one or more): information system process; role; user] associated with the review, analysis, and reporting of audit information."

Cause:

FLRA did not appropriate the required time to review the audit logs.

Effect:

Without appropriate audit log reviews, there is the risk that inadvertent or adverse actions will go undetected and thereby cause harm to the agency.

Recommendation:

5. Ensure audit log reviews occur at least monthly.

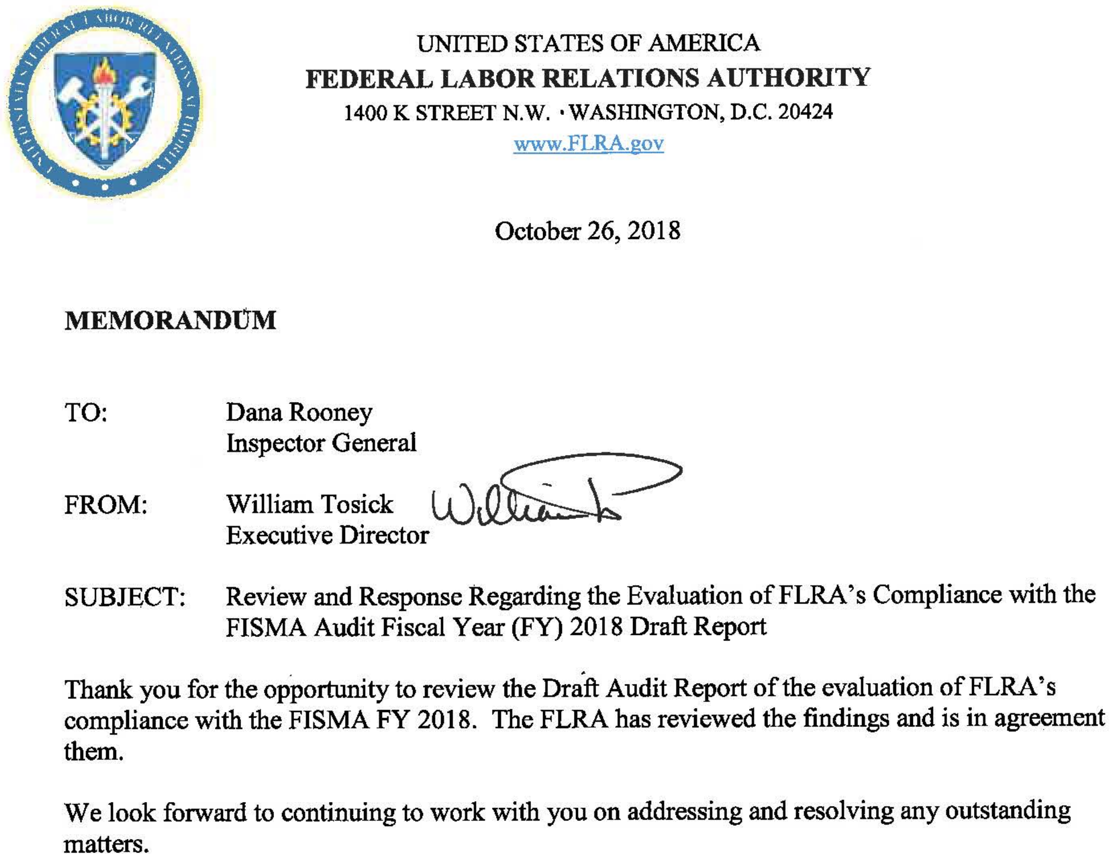
Management Response:

Management agrees with our recommendation.

Appendix 2
Prior Year Recommendation

#	Year Initiated	POA&M	Open / Closed
1	2015	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.	Closed

Appendix 3
Management Response



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

October 26, 2018

MEMORANDUM

TO: Dana Rooney
Inspector General

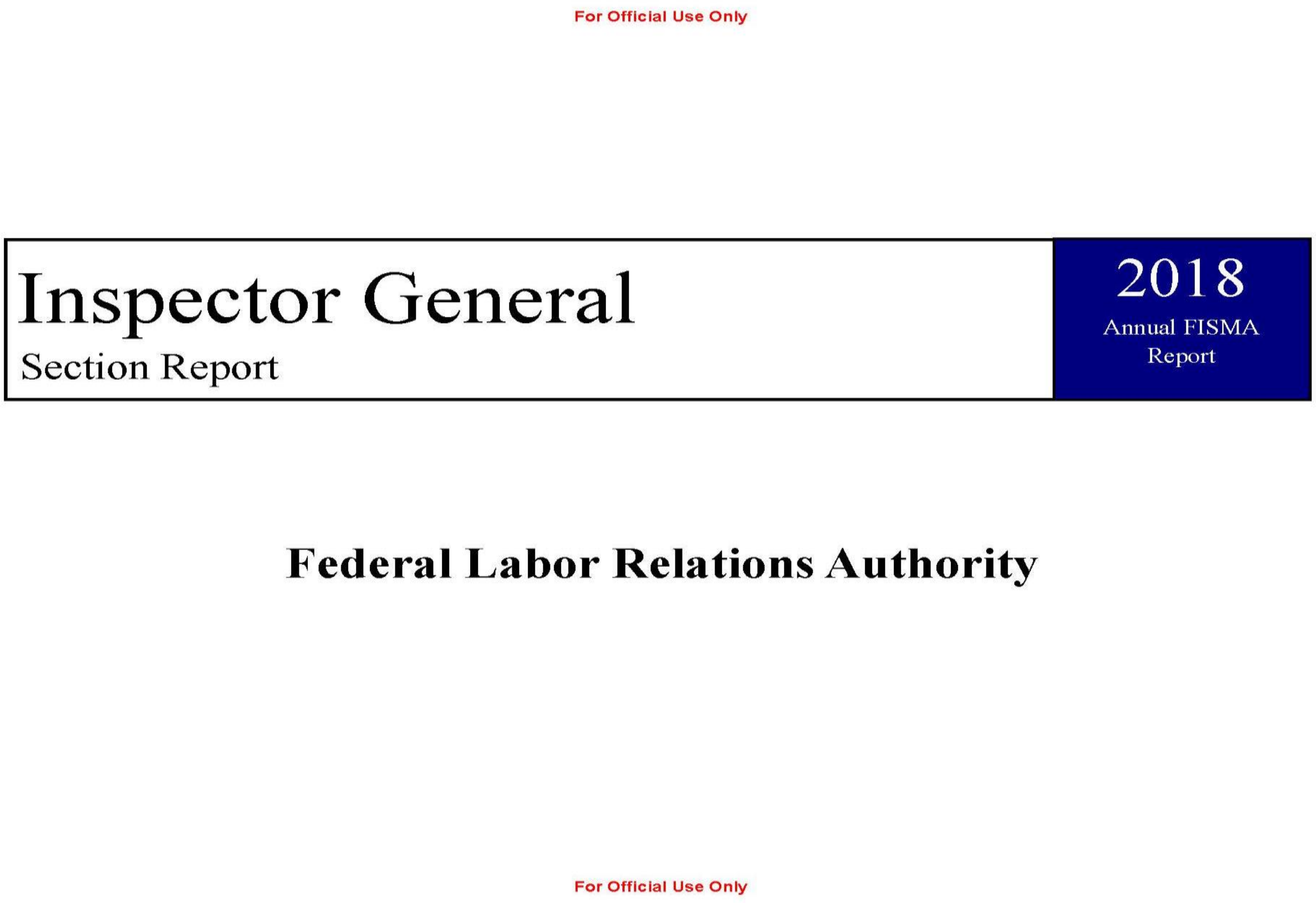
FROM: William Tosick William
Executive Director

SUBJECT: Review and Response Regarding the Evaluation of FLRA's Compliance with the FISMA Audit Fiscal Year (FY) 2018 Draft Report

Thank you for the opportunity to review the Draft Audit Report of the evaluation of FLRA's compliance with the FISMA FY 2018. The FLRA has reviewed the findings and is in agreement them.

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

Appendix 4
OIG Responses Reported in Cyberscope



For Official Use Only

Inspector General

Section Report

2018

Annual FISMA

Report

Federal Labor Relations Authority

For Official Use Only

Function 1: Identify - Risk Management

1 To what extent does the organization maintain a comprehensive and accurate inventory of its information systems (including cloud systems, public facing websites, and third party systems), and system interconnections (NIST SP 800-53: CA-3, PM-5, and CM-8; OMB M-04-25; NIST 800-161; NIST Cybersecurity Framework (CSF): ID.AM-1 – 4; FY 2018 CIO FISMA Metrics: 1.1, 1.4, and 1.5)?

Consistently Implemented (Level 3)

Comments: Please refer to our FISMA audit report, which details all of the deficiencies.

2 To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets connected to the organization's network with the detailed information necessary for tracking and reporting (NIST SP 800-53: CA-7 and CM-8; NIST SP 800-137; Federal Enterprise Architecture (FEA) Framework, v2; FY 2018 CIO FISMA Metrics: 1.2)?

Consistently Implemented (Level 3)

Comments: Please refer to our FISMA audit report, which details all of the deficiencies.

3 To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of the software and associated licenses used within the organization with the detailed information necessary for tracking and reporting (NIST SP 800-53: CA-7, CM-8, and CM-10; NIST SP 800-137; FEA Framework, v2)?

Consistently Implemented (Level 3)

Comments: Please refer to our FISMA audit report, which details all of the deficiencies.

4 To what extent has the organization categorized and communicated the importance/priority of information systems in enabling its missions and business functions (NIST SP 800-53: RA-2, PM-7, and PM-11; NIST SP 800-60; CSF: ID.BE-3; FIPS 199; FY 2018 CIO FISMA Metrics: 1.1)?

Consistently Implemented (Level 3)

5 To what extent has the organization established, communicated, and implemented its risk management policies, procedures, and strategy that includes the organization’s processes and methodologies for categorizing risk, developing a risk profile, assessing risk, risk appetite/tolerance levels, responding to risk, and monitoring risk (NIST SP 800-39; NIST SP 800-53: PM-8, PM-9; CSF: ID RM-1 – ID.RM-3; OMB A-123; OMB M-16-17; Green Book (Principle #6); CFO Council ERM Playbook; OMB M-17-25; FY 2018 CIO FISMA Metrics: 1.6)?

Consistently Implemented (Level 3)

Comments: Please refer to our FISMA audit report, which details all of the deficiencies.

Function 1: Identify - Risk Management

6 To what extent does the organization utilize an information security architecture to provide a disciplined and structured methodology for managing risk, including risk from the organization's supply chain (NIST SP 800-39; FEA Framework; NIST SP 800-53: PL-8, SA-3, SA-8, SA-9, SA-12, and PM-9; NIST SP 800-161; DHS Binding Operational Directive 17-01)?

Ad Hoc (Level 1)

Comments: Please refer to our FISMA audit report, which details all of the deficiencies.

7 To what degree have roles and responsibilities of stakeholders involved in risk management, including the risk executive function/Chief Risk Officer/Senior Accountable Official for Risk Management, Chief Information Officer, Chief Information Security Officer, and other internal and external stakeholders and mission specific resources been defined and communicated across the organization (NIST SP 800-39: Section 2.3.1 and 2.3.2; NIST SP 800-53: RA-1; CSF: ID.RM-1 – ID.GV-2; OMB A-123; CFO Council ERM Playbook)?

Consistently Implemented (Level 3)

Comments: Please refer to our FISMA audit report, which details all of the deficiencies.

8 To what extent has the organization ensured that plans of action and milestones (POA&Ms) are utilized for effectively mitigating security weaknesses (NIST SP 800-53: CA-5; OMB M-04-25)?

Consistently Implemented (Level 3)

Comments: Please refer to our FISMA audit report, which details all of the deficiencies.

9 To what extent has the organization defined, communicated, and implemented its policies and procedures for conducting system level risk assessments, including for identifying and prioritizing
(i) internal and external threats, including through use of the common vulnerability scoring system, or other equivalent framework
(ii) internal and external asset vulnerabilities, including through vulnerability scanning,
(iii) the potential likelihoods and business impacts/consequences of threats exploiting vulnerabilities, and
(iv) security controls to mitigate system-level risks (NIST SP 800-37; NIST SP 800-39; NIST SP 800-53: PL-2 and RA-1; NIST SP 800-30; CSF:ID.RA-1 – 6)?

Managed and Measurable (Level 4)

10 To what extent does the organization ensure that information about risks are communicated in a timely manner to all necessary internal and external stakeholders (CFO Council ERM Playbook; OMB A-123; OMB Circular A-11; Green Book (Principles #9, #14 and #15))?

Managed and Measurable (Level 4)

Function 1: Identify - Risk Management

11 To what extent does the organization ensure that specific contracting language (such as appropriate information security and privacy requirements and material disclosures, FAR clauses, and clauses on protection, detection, and reporting of information) and SLAs are included in appropriate contracts to mitigate and monitor the risks related to contractor systems and services (FAR Case 2007-004; Common Security Configurations; FAR Sections: 24.104, 39.101, 39.105, 39.106, and 52.239-1; President's Management Council; NIST SP 800-53: SA-4; FedRAMP standard contract clauses; Cloud Computing Contract Best Practices; FY 2018 CIO FISMA Metrics: 1.5; Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure)?

Consistently Implemented (Level 3)

Comments: Please refer to our FISMA audit report, which details all of the deficiencies.

12 To what extent does the organization utilize technology (such as a governance, risk management, and compliance tool) to provide a centralized, enterprise wide (portfolio) view of risks across the organization, including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards (NIST SP 800-39; OMB A-123; CFO Council ERM Playbook)?

Ad Hoc (Level 1)

Comments: Please refer to our FISMA audit report, which details all of the deficiencies.

13.1 Please provide the assessed maturity level for the agency's Identify - Risk Management function.

Consistently Implemented (Level 3)

Comments: Please refer to our FISMA audit report, which details all of the deficiencies.

13.2 Provide any additional information on the effectiveness (positive or negative) of the organization's risk management program that was not noted in the questions above. Taking into consideration the overall maturity level generated from the questions above and based on all testing performed, is the risk management program effective?

Please refer to our FISMA audit report, which details all of the deficiencies.

Calculated Maturity Level - Consistently Implemented (Level 3)

Function 2A: Protect - Configuration Management

14 To what degree have the roles and responsibilities of configuration management stakeholders been defined, communicated across the agency, and appropriately resourced (NIST SP 800-53: CM-1; NIST SP 800-128: Section 2.4)?

Ad Hoc (Level 1)

Function 2A: Protect - Configuration Management

15 To what extent does the organization utilize an enterprise wide configuration management plan that includes, at a minimum, the following components: roles and responsibilities, including establishment of a Change Control Board (CCB) or related body; configuration management processes, including processes for: identifying and managing configuration items during the appropriate phase within an organization's SDLC; configuration monitoring; and applying configuration management requirements to contractor operated systems (NIST SP 800-128: Section 2.3.2; NIST SP 800-53: CM-9)?

Ad Hoc (Level 1)

Comments: Please refer to our FISMA audit report, which details all of the deficiencies.

16 To what degree have information system configuration management policies and procedures been defined and implemented across the organization? (Note: the maturity level should take into consideration the maturity of questions 17, 18, 19, and 21) (NIST SP 800-53: CM-1; NIST SP 800-128: 2.2.1)?

Managed and Measurable (Level 4)

17 To what extent does the organization utilize baseline configurations for its information systems and maintain inventories of related components at a level of granularity necessary for tracking and reporting (NIST SP 800-53: CM-2 and CM-8; FY 2018 CIO FISMA Metrics: 1.1 and 2.2; CSF: ID.DE.CM-7)?

Managed and Measurable (Level 4)

18 To what extent does the organization utilize configuration settings/common secure configurations for its information systems? (NIST SP 800-53: CM-6, CM-7, and SI-2; FY 2018 CIO FISMA Metrics: 1.1 and 2.2; SANS/CIS Top 20 Security Controls 3.7)?

Defined (Level 2)

Comments: Please refer to our FISMA audit report, which details all of the deficiencies.

19 To what extent does the organization utilize flaw remediation processes, including patch management, to manage software vulnerabilities (NIST SP 800-53: CM-3 and SI-2; NIST SP 800-40, Rev. 3; OMB M-16-04; SANS/CIS Top 20, Control 4.5; FY 2018 CIO FISMA Metrics: 2.13; and DHS Binding Operational Directive 15-01)?

Consistently Implemented (Level 3)

Comments: Please refer to our FISMA audit report, which details all of the deficiencies.

20 To what extent has the organization adopted the Trusted Internet Connection (TIC) program to assist in protecting its network (OMB M-08-05)?

Defined (Level 2)

Function 2A: Protect - Configuration Management

21 To what extent has the organization defined and implemented configuration change control activities including: determination of the types of changes that are configuration controlled; review and approval/disapproval of proposed changes with explicit consideration of security impacts and security classification of the system; documentation of configuration change decisions; implementation of approved configuration changes; retaining records of implemented changes; auditing and review of configuration changes; and coordination and oversight of changes by the CCB, as appropriate (NIST SP 800-53: CM-2 and CM-3)?

Consistently Implemented (Level 3)

Comments: Please refer to our FISMA audit report, which details all of the deficiencies.

22 Provide any additional information on the effectiveness (positive or negative) of the organization's configuration management program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the configuration management program effective?

Please refer to our FISMA audit report, which details all of the deficiencies.

Calculated Maturity Level - Managed and Measurable (Level 4)

Function 2B: Protect - Identity and Access Management

23 To what degree have the roles and responsibilities of identity, credential, and access management (ICAM) stakeholders been defined, communicated across the agency, and appropriately resourced (NIST SP 800-53: AC-1, IA-1, and PS-1; Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance (FICAM))?

Consistently Implemented (Level 3)

24 To what degree does the organization utilize an ICAM strategy to guide its ICAM processes and activities (FICAM)?

Defined (Level 2)

Comments: Please refer to our FISMA audit report, which details all of the deficiencies.

25 To what degree have ICAM policies and procedures been defined and implemented? (Note: the maturity level should take into consideration the maturity of questions 26 through 31) (NIST SP 800-53: AC-1 and IA-1; Cybersecurity Strategy and Implementation Plan (CSIP); SANS/CIS Top 20: 14.1; FY 2018 CIO FISMA Metrics: 2.3).

Defined (Level 2)

Comments: Please refer to our FISMA audit report, which details all of the deficiencies.

Function 2B: Protect - Identity and Access Management

26 To what extent has the organization developed and implemented processes for assigning personnel risk designations and performing appropriate screening prior to granting access to its systems (NIST SP 800-53: PS-2 and PS-3; National Insider Threat Policy; FY 2018 CIO FISMA Metrics: 2.16)?

Consistently Implemented (Level 3)

Comments: Please refer to our FISMA audit report, which details all of the deficiencies.

27 To what extent does the organization ensure that access agreements, including nondisclosure agreements, acceptable use agreements, and rules of behavior, as appropriate, for individuals (both privileged and non-privileged users) that access its systems are completed and maintained (NIST SP 800-53: AC-8, PL-4, and PS-6)?

Consistently Implemented (Level 3)

Comments: Please refer to our FISMA audit report, which details all of the deficiencies.

28 To what extent has the organization implemented strong authentication mechanisms (two-factor PIV credential or other NIST 800-63 r3 Identity Assurance Level (IAL)3/ Authenticator Assurance Level (AAL) 3/ Federated Assurance Level (FAL) 3 credential) for non-privileged users to access the organization's facilities, networks, and systems, including for remote access (CSIP; HSPD-12; NIST SP 800-53: AC-17; NIST SP 800-128; FIPS 201-2; NIST SP 800-63; FY 2018 CIO FISMA Metrics: 2.4; and Cybersecurity Sprint)?

Consistently Implemented (Level 3)

Comments: Please refer to our FISMA audit report, which details all of the deficiencies.

29 To what extent has the organization implemented strong authentication mechanisms (two-factor PIV credential or other NIST 800-63 r3 IAL 3/ AAL 3/ FAL 3 credential) for privileged users to access the organization's facilities, networks, and systems, including for remote access (CSIP; HSPD-12; NIST SP 800-53: AC-17; NIST SP 800-128; FIPS 201-2; NIST SP 800-63; FY 2018 CIO FISMA Metrics: 2.5; and Cybersecurity Sprint)?

Consistently Implemented (Level 3)

Comments: Please refer to our FISMA audit report, which details all of the deficiencies.

30 To what extent does the organization ensure that privileged accounts are provisioned, managed, and reviewed in accordance with the principles of least privilege and separation of duties? Specifically, this includes processes for periodic review and adjustment of privileged user accounts and permissions, inventorying and validating the scope and number of privileged accounts, and ensuring that privileged user account activities are logged and periodically reviewed (FY 2018 CIO FISMA Metrics: 2.4 and 2.5; NIST SP 800-53: AC-1, AC-2 (2), and AC-17; CSIP)?

Consistently Implemented (Level 3)

Comments: Please refer to our FISMA audit report, which details all of the deficiencies.

Function 2B: Protect - Identity and Access Management

31 To what extent does the organization ensure that appropriate configuration/connection requirements are maintained for remote access connections? This includes the use of appropriate cryptographic modules, system time-outs, and the monitoring and control of remote access sessions (NIST SP 800-53: AC-17 and SI-4; and FY 2018 CIO FISMA Metrics: 2.10)?

Consistently Implemented (Level 3)

Comments: Please refer to our FISMA audit report, which details all of the deficiencies.

32 Provide any additional information on the effectiveness (positive or negative) of the organization's identity and access management program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the identity and access management program effective?

Please refer to our FISMA audit report, which details all of the deficiencies.

Calculated Maturity Level - Consistently Implemented (Level 3)

Function 2C: Protect - Data Protection and Privacy

33 To what extent has the organization developed a privacy program for the protection of personally identifiable information (PII) that is collected, used, maintained, shared, and disposed of by information systems (NIST SP 800-122; OMB M-18-02; OMB A-130, Appendix I; NIST SP 800-53: AR-4 and Appendix J)?

Consistently Implemented (Level 3)

Comments: Please refer to our FISMA audit report, which details all of the deficiencies.

34 To what extent has the organization implemented the following security controls to protect its PII and other agency sensitive data, as appropriate, throughout the data lifecycle? (NIST SP 800-53; Appendix J, SC-8, SC-28, MP-3, and MP-6; FY 2018 CIO FISMA Metrics: 2.9 and 2.10)?

Encryption of data at rest

Encryption of data in transit

Limitation of transfer to removable media

Sanitization of digital media prior to disposal or reuse

Managed and Measurable (Level 4)

35 To what extent has the organization implemented security controls to prevent data exfiltration and enhance network defenses? (NIST SP 800-53: SI-3, SI-7(8), SI-4(4) and (18), SC-7(10), and SC-18; FY 2018 CIO FISMA Metrics: 3.8 – 3.12)?

Consistently Implemented (Level 3)

Comments: Please refer to our FISMA audit report, which details all of the deficiencies.

Function 2C: Protect - Data Protection and Privacy

36 To what extent has the organization developed and implemented a Data Breach Response Plan, as appropriate, to respond to privacy events? (NIST SP 800-122; NIST SP 800-53: Appendix J, SE-2; FY 2018 SAOP FISMA metrics; OMB M-17-12; and OMB M-17-25)?

Consistently Implemented (Level 3)

Comments: Please refer to our FISMA audit report, which details all of the deficiencies.

37 To what degree does the organization ensure that privacy awareness training is provided to all individuals, including role-based privacy training (NIST SP 800-53: AR-5)? (Note: Privacy awareness training topics should include, as appropriate: responsibilities under the Privacy Act of 1974 and E-Government Act of 2002, consequences for failing to carry out responsibilities, identifying privacy risks, mitigating privacy risks, and reporting privacy incidents, data collections and use requirements)?

Consistently Implemented (Level 3)

Comments: Please refer to our FISMA audit report, which details all of the deficiencies.

38 Provide any additional information on the effectiveness (positive or negative) of the organization's data protection and privacy program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the data protection and privacy program effective?

Please refer to our FISMA audit report, which details all of the deficiencies.

Calculated Maturity Level - Consistently Implemented (Level 3)

Function 2D: Protect - Security Training

39 To what degree have the roles and responsibilities of security awareness and training program stakeholders been defined, communicated across the agency, and appropriately resourced? (Note: this includes the roles and responsibilities for the effective establishment and maintenance of an organization wide security awareness and training program as well as the awareness and training related roles and responsibilities of system users and those with significant security responsibilities (NIST SP 800-53: AT-1; and NIST SP 800-50).

Consistently Implemented (Level 3)

40 To what extent does the organization utilize an assessment of the skills, knowledge, and abilities of its workforce to provide tailored awareness and specialized security training within the functional areas of: identify, protect, detect, respond, and recover (NIST SP 800-53: AT-2 and AT-3; NIST SP 800-50: Section 3.2; Federal Cybersecurity Workforce Assessment Act of 2015; National Cybersecurity Workforce Framework v1.0; NIST SP 800-181; and CIS/SANS Top 20: 17.1)?

Consistently Implemented (Level 3)

Comments: Please refer to our FISMA audit report, which details all of the deficiencies.

Function 2D: Protect - Security Training

41 To what extent does the organization utilize a security awareness and training strategy/plan that leverages its organizational skills assessment and is adapted to its culture? (Note: the strategy/plan should include the following components: the structure of the awareness and training program, priorities, funding, the goals of the program, target audiences, types of courses/material for each audience, use of technologies (such as email advisories, intranet updates/wiki pages/social media, web based training, phishing simulation tools), frequency of training, and deployment methods (NIST SP 800-53: AT-1; NIST SP 800-50: Section 3).

Managed and Measurable (Level 4)

42 To what degree have security awareness and specialized security training policies and procedures been defined and implemented? (Note: the maturity level should take into consideration the maturity of questions 43 and 44 below) (NIST SP 800-53: AT-1 through AT-4; and NIST SP 800-50).

Managed and Measurable (Level 4)

43 To what degree does the organization ensure that security awareness training is provided to all system users and is tailored based on its organizational requirements, culture, and types of information systems? (Note: awareness training topics should include, as appropriate: consideration of organizational policies, roles and responsibilities, secure e-mail, browsing, and remote access practices, mobile device security, secure use of social media, phishing, malware, physical security, and security incident reporting (NIST SP 800-53: AT-2; FY 2018 CIO FISMA Metrics: 2.15; NIST SP 800-50: 6.2; SANS Top 20: 17.4).

Managed and Measurable (Level 4)

44 To what degree does the organization ensure that specialized security training is provided to all individuals with significant security responsibilities (as defined in the organization's security policies and procedures) (NIST SP 800-53: AT-3 and AT-4; FY 2018 CIO FISMA Metrics: 2.15)?

Managed and Measurable (Level 4)

45.1 Please provide the assessed maturity level for the agency's Protect Function.

Managed and Measurable (Level 4)

45.2 Provide any additional information on the effectiveness (positive or negative) of the organization’s security training program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the security training program effective?

Please refer to our FISMA audit report, which details all of the deficiencies.

Calculated Maturity Level - Managed and Measurable (Level 4)

Function 3: Detect - ISCM

Function 3: Detect - ISCM

46 To what extent does the organization utilize an information security continuous monitoring (ISCM) strategy that addresses ISCM requirements and activities at each organizational tier and helps ensure an organization-wide approach to ISCM (NIST SP 800-137: Sections 3.1 and 3.6)?

Managed and Measurable (Level 4)

47 To what extent does the organization utilize ISCM policies and procedures to facilitate organization-wide, standardized processes in support of the ISCM strategy? ISCM policies and procedures address, at a minimum, the following areas: ongoing assessments and monitoring of security controls; collection of security related information required for metrics, assessments, and reporting; analyzing ISCM data, reporting findings, and reviewing and updating the ISCM strategy (NIST SP 800-53: CA-7) (Note: The overall maturity level should take into consideration the maturity of question 49)?

Managed and Measurable (Level 4)

48 To what extent have ISCM stakeholders and their roles, responsibilities, levels of authority, and dependencies been defined and communicated across the organization (NIST SP 800-53: CA-1; NIST SP 800-137; and FY 2018 CIO FISMA Metrics)?

Managed and Measurable (Level 4)

49 How mature are the organization's processes for performing ongoing assessments, granting system authorizations, and monitoring security controls (NIST SP 800-137: Section 2.2; NIST SP 800-53: CA-2, CA-6, and CA-7; NIST Supplemental Guidance on Ongoing Authorization; OMB M-14-03)?

Managed and Measurable (Level 4)

50 How mature is the organization's process for collecting and analyzing ISCM performance measures and reporting findings (NIST SP 800-137)?

Managed and Measurable (Level 4)

51.1 Please provide the assessed maturity level for the agency's Detect - ISCM function.

Managed and Measurable (Level 4)

51.2 Provide any additional information on the effectiveness (positive or negative) of the organization's ISCM program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the ISCM program effective?

Please refer to our FISMA audit report, which details all of the deficiencies.

Calculated Maturity Level - Managed and Measurable (Level 4)

Function 4: Respond - Incident Response

Function 4: Respond - Incident Response

52 To what extent has the organization defined and implemented its incident response policies, procedures, plans, and strategies, as appropriate, to respond to cybersecurity events (NIST SP 800-53: IR-1; NIST SP 800-61 Rev. 2; NIST SP 800-184; OMB M-17-25; OMB M-17-09; FY 2018 CIO FISMA Metrics: 4.1, 4.3, 4.6, and 5.3; Presidential Policy Direction (PPD) 41)? (Note: The overall maturity level should take into consideration the maturity of questions 53 - 58)?

Consistently Implemented (Level 3)

Comments: Please refer to our FISMA audit report, which details all of the deficiencies.

53 To what extent have incident response team structures/models, stakeholders, and their roles, responsibilities, levels of authority, and dependencies been defined and communicated across the organization (NIST SP 800-53: IR-7; NIST SP 800-83; NIST SP 800-61 Rev. 2; OMB M-18-02; OMB M-16-04; FY 2018 CIO FISMA Metrics: Section 4; and US-CERT Federal Incident Notification Guidelines)?

Consistently Implemented (Level 3)

Comments: Please refer to our FISMA audit report, which details all of the deficiencies.

54 How mature are the organization's processes for incident detection and analysis? (NIST 800-53: IR-4 and IR-6; NIST SP 800-61 Rev. 2; OMB M-18-02; and US-CERT Incident Response Guidelines)?

Consistently Implemented (Level 3)

Comments: Please refer to our FISMA audit report, which details all of the deficiencies.

55 How mature are the organization's processes for incident handling (NIST 800-53: IR-4; NIST SP 800-61, Rev. 2)?

Consistently Implemented (Level 3)

Comments: Please refer to our FISMA audit report, which details all of the deficiencies.

56 To what extent does the organization ensure that incident response information is shared with individuals with significant security responsibilities and reported to external stakeholders in a timely manner (FISMA; OMB M-18-02; NIST SP 800-53: IR-6; US-CERT Incident Notification Guidelines; PPD-41; DHS Cyber Incident Reporting Unified Message)?

Consistently Implemented (Level 3)

Comments: Please refer to our FISMA audit report, which details all of the deficiencies.

Function 4: Respond - Incident Response

57 To what extent does the organization collaborate with stakeholders to ensure on-site, technical assistance/surge capabilities can be leveraged for quickly responding to incidents, including through contracts/agreements, as appropriate, for incident response support (FY 2018 CIO FISMA Metrics: 4.4; NIST SP 800-86; NIST SP 800-53: IR-4; OMB M-18-02; PPD-41).

Defined (Level 2)

Comments: Please refer to our FISMA audit report, which details all of the deficiencies.

58 To what degree does the organization utilize the following technology to support its incident response program?

Web application protections, such as web application firewalls

Event and incident management, such as intrusion detection and prevention tools, and incident tracking and reporting tools

Aggregation and analysis, such as security information and event management (SIEM) products

Malware detection, such as antivirus and antispam software technologies

Information management, such as data loss prevention

File integrity and endpoint and server security tools (NIST SP 800-137; NIST SP 800-61, Rev. 2; NIST SP 800-44)

Defined (Level 2)

Comments: Please refer to our FISMA audit report, which details all of the deficiencies.

59.1 Please provide the assessed maturity level for the agency's Respond - Incident Response function.

Consistently Implemented (Level 3)

Comments: Please refer to our FISMA audit report, which details all of the deficiencies.

59.2 Provide any additional information on the effectiveness (positive or negative) of the organization's incident response program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the incident response program effective?

Please refer to our FISMA audit report, which details all of the deficiencies.

Calculated Maturity Level - Consistently Implemented (Level 3)

Function 5: Recover - Contingency Planning

Function 5: Recover - Contingency Planning

60 To what extent have roles and responsibilities of stakeholders involved in information systems contingency planning been defined and communicated across the organization, including appropriate delegations of authority (NIST SP 800-53: CP-1 and CP-2; NIST SP 800-34; NIST SP 800-84; FCD-1: Annex B)?

Consistently Implemented (Level 3)

61 To what extent has the organization defined and implemented its information system contingency planning program through policies, procedures, and strategies, as appropriate (Note: Assignment of an overall maturity level should take into consideration the maturity of questions 62-66) (NIST SP 800-34; NIST SP 800-161; FY 2018 CIO FISMA Metrics: 5.1, 5.2, and 5.5).

Consistently Implemented (Level 3)

Comments: Please refer to our FISMA audit report, which details all of the deficiencies.

62 To what degree does the organization ensure that the results of business impact analyses are used to guide contingency planning efforts (NIST SP 800-53: CP-2; NIST SP 800-34, Rev. 1, 3.2; FIPS 199; FCD-1; OMB M-17-09; FY 2018 CIO FISMA Metrics: 5.6)?

Defined (Level 2)

63 To what extent does the organization ensure that information system contingency plans are developed, maintained, and integrated with other continuity plans (NIST SP 800-53: CP-2; NIST SP 800-34; FY 2018 CIO FISMA Metrics: 5.1, 5.2, and 5.5)?

Consistently Implemented (Level 3)

Comments: Please refer to our FISMA audit report, which details all of the deficiencies.

64 To what extent does the organization perform tests/exercises of its information system contingency planning processes (NIST SP 800-34; NIST SP 800-53: CP-3 and CP-4; FY 2018 CIO FISMA Metrics: 5.1, 5.2, and 5.5)?

Consistently Implemented (Level 3)

Comments: Please refer to our FISMA audit report, which details all of the deficiencies.

65 To what extent does the organization perform information system backup and storage, including use of alternate storage and processing sites, as appropriate (NIST SP 800-53: CP-6, CP-7, CP-8, and CP-9; NIST SP 800-34: 3.4.1, 3.4.2, 3.4.3; FCD-1; NIST CSF: PR.IP-4; FY 2018 CIO FISMA Metrics: 5.4; and NARA guidance on information systems security records)?

Consistently Implemented (Level 3)

Comments: Please refer to our FISMA audit report, which details all of the deficiencies.

Function 5: Recover - Contingency Planning

66 To what level does the organization ensure that information on the planning and performance of recovery activities is communicated to internal stakeholders and executive management teams and used to make risk based decisions (CSF: RC.CO-3; NIST SP 800-53: CP-2 and IR-4)?

Consistently Implemented (Level 3)

Comments: Please refer to our FISMA audit report, which details all of the deficiencies.

67.1 Please provide the assessed maturity level for the agency's Recover - Contingency Planning function.

Consistently Implemented (Level 3)

Comments: Please refer to our FISMA audit report, which details all of the deficiencies.

67.1 Please provide the assessed maturity level for the agency's Recover - Contingency Planning function.

Consistently Implemented (Level 3)

67.2 Provide any additional information on the effectiveness (positive or negative) of the organization’s contingency planning program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the contingency program effective?

Please refer to our FISMA audit report, which details all of the deficiencies.

Calculated Maturity Level - Consistently Implemented (Level 3)

Comments: Please refer to our FISMA audit report, which details all of the deficiencies.

Function 0: Overall

0.1 Please provide an overall IG self-assessment rating (Effective/Not Effective)

Effective

0.2 Please provide an overall assessment of the agency's information security program. The narrative should include a description of the assessment scope, a summary on why the information security program was deemed effective/ineffective and any recommendations on next steps. Please note that OMB will include this information in the publicly available Annual FISMA Report to Congress to provide additional context for the Inspector General's effectiveness rating of the agency's information security program. OMB may modify the response to conform with the grammatical and narrative structure of the Annual Report.

Please refer to our FISMA audit report, which details all of the deficiencies.

APPENDIX A: Maturity Model Scoring

Function 1: Identify - Risk Management

Function	Count
Ad-Hoc	2
Defined	0
Consistently Implemented	8
Managed and Measurable	2
Optimized	0
Function Rating: Consistently Implemented (Level 3)Not Effective	0

Function 2A: Protect - Configuration Management

Function	Count
Ad-Hoc	2
Defined	2
Consistently Implemented	2
Managed and Measurable	2
Optimized	0
Function Rating: Managed and Measurable (Level 4)Effective	0

Function 2B: Protect - Identity and Access Management

Function	Count
Ad-Hoc	0
Defined	2
Consistently Implemented	7
Managed and Measurable	0
Optimized	0
Function Rating: Consistently Implemented (Level 3)Not Effective	0

Function 2C: Protect - Data Protection and Privacy

Function	Count
Ad-Hoc	0
Defined	0
Consistently Implemented	4
Managed and Measurable	1
Optimized	0
Function Rating: Consistently Implemented (Level 3)Not Effective	0

Function 2D: Protect - Security Training

Function	Count
Ad-Hoc	0
Defined	0
Consistently Implemented	2
Managed and Measurable	4
Optimized	0
Function Rating: Managed and Measurable (Level 4)Effective	0

Function 3: Detect - ISCM

Function	Count
Ad-Hoc	0
Defined	0
Consistently Implemented	0
Managed and Measurable	5
Optimized	0
Function Rating: Managed and Measurable (Level 4)Effective	0

Function 4: Respond - Incident Response

Function	Count
Ad-Hoc	0
Defined	2
Consistently Implemented	5
Managed and Measurable	0
Optimized	0
Function Rating: Consistently Implemented (Level 3)Not Effective	0

Function 5: Recover - Contingency Planning

Function	Count
Ad-Hoc	0
Defined	1
Consistently Implemented	6
Managed and Measurable	0
Optimized	0
Function Rating: Consistently Implemented (Level 3)Not Effective	0

Maturity Levels by Function

Function	Calculated Maturity Level	Assessed Maturity Level	Explanation
Function 1: Identify - Risk Management	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	Please refer to our FISMA audit report, which details all of the deficiencies.
Function 2: Protect - Configuration Management / Identity & Access Management / Data Protection & Privacy / Security Training	Managed and Measurable (Level 4)	Managed and Measurable (Level 4)	
Function 3: Detect - ISCM	Managed and Measurable (Level 4)	Managed and Measurable (Level 4)	
Function 4: Respond - Incident Response	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	Please refer to our FISMA audit report, which details all of the deficiencies.
Function 5: Recover - Contingency Planning	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	Please refer to our FISMA audit report, which details all of the deficiencies.
Overall	Not Effective	Effective	Please refer to our FISMA audit report, which details all of the deficiencies.

Appendix 5
Report Distribution

Federal Labor Relations Authority

Ernest DuBester, Member
James Abbott, Member
William Tosick, Executive Director
Michael Jeffries, Chief Information Officer
Fred Jacob, Solicitor

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