Office of Inspector General

FISMA Evaluation

EVALUATION OF THE FEDERAL LABOR RELATIONS AUTHORITY COMPLIANCE WITH THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT OF 2014

Fiscal Year 2017

Report No. MAR-18-01

October 2017

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

CONTENTS

Evaluation Report

Results in Brief 1
Background 1
Scope and Methodology 2

Appendices

Appendix 1: Prior Year Recommendations 3
Appendix 2: Management Response 4
Appendix 3: OIG Responses Reported in Cyberscope 6
Appendix 4: Report Distribution 7

Abbreviations

Dembo Jones	Dembo Jones, P.C.
FISMA	Federal Information Security Modernization Act
FLRA	Federal Labor Relations Authority
FY	Fiscal Year
GSS	General Support System
IG	Inspector General
IT	Information Technology
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
SCAs	Security Controls Assessments
SP	NIST Special Publication Series
SSPs	System Security Plans

Evaluation of FLRA's Compliance with the FISMA FY 2017

Report No. MAR-18-01 ***October 25, 2017***

The Honorable Patrick Pizzella
Acting 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) 2017 report to the Office of Management and Budget (OMB) and Congress.

Results in Brief

During our FY 2017 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 were a total of 5 prior recommendations, of which 1 is still open. There are no new findings.

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 1for 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.

6010 Executive Blvd • Suite 900
Rockville, MD 20852
P 301.770.5100 • F 301.770.5202

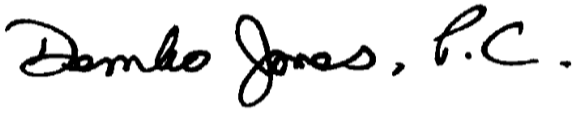
Dembo Jones, P.C.
A Member of Allinial Global
www.dembojones.com

8850 Stanford Blvd • Suite 2000
Columbia, MD 21045
P 410.290.0770 • F 410.290.0774

Under FISMA, agency heads are responsible for providing information security protections commensurate with the risk and magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems. FISMA directs Federal agencies to report annually to the OMB Director, Comptroller General, and selected congressional committees on the adequacy and effectiveness of agency information security policies, procedures, and practices and compliance with FISMA. In addition, FISMA requires agencies to have an annual independent evaluation performed of their information security programs and practices and to report the evaluation results to OMB. FISMA states that the independent evaluation is to be performed by the agency IG or an independent external auditor as determined by the IG. Implementing adequate information security controls is essential to ensuring an organization can effectively meet its mission. The IG plays an essential role in supporting Federal agencies in identifying areas for improvement. In support of that critical goal the FLRA supports the development of a strategy to secure the FLRA computing environment which centers on providing confidentially, integrity, and availability.

Scope and Methodology

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



Dembo Jones, P.C.

Rockville, Maryland
October 25, 2017

Appendix 1
Prior Year Recommendations

#	Year Initiated	POA&M	Open / Closed
1	2014	1. All controls within NIST 800-53 Revision 4 for the systems' categorization should be used as a starting point for determining the assessments and implementation of a continuous monitoring program. Then, management should determine which of those controls are critical. Those critical controls should be assessed every year. The remainder of the controls should then be divided by three and then assessed over a three-year period, whereby 1/3 of the remaining controls are assessed each year. Ideally, the controls to be assessed each year should then be done on a quarterly basis by taking the annual set of controls and assessing ¼ each quarter. Upon completion of continuous monitoring, the agency should maintain metrics such as number of controls assessed on a monthly basis, number of deficiencies by family, etc.	Closed
2	2014	2. Ensure any deficiencies as a result of the continuous monitoring assessments will be clearly and timely reported as a POA&M.	Closed
3	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.	Open
4	2015	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.	Closed
5	2015	3. On an annual basis, all FLRA employees should have their access reviewed to ensure it 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.	Closed

Appendix 2
Management Response

UNITED STATES OF AMERICA

FEDERAL LABOR RELATIONS AUTHORITY

October 25, 2017

MEMORANDUM

TO: Dana Rooney
Inspector General

FROM: Michael Jeffries
Acting Executive Director

SUBJECT: Follow-up Response and Action Plan Regarding Compliance with the Federal Information Security Management Act (FISMA) Fiscal Year (FY) 2017 Report

Thank you for the opportunity to review and provide a follow-up memo addressing the FISMA FY17 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 one remaining vulnerability.

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

#	Finding	Management Response	Corrective Timeline
1	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 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 assessed each year should then 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.	The FLRA IRMD Staff reviewed all NIST 800-53 Revision 4 controls as part of their IT security plan update/review. IRMD has developed a continuous plan where they review all risk categorized as "high" annually and the remaining split over a three year period with quarterly reviews. This will ensure all controls are reviewed over the three years as recommended. The updated SSP spreadsheet was submitted to Auditor.	Closed
2	Ensure any deficiencies as a result of the continuous monitoring assessments will be clearly and timely reported as POA&M.	The FLRA IRMD Staff are actively monitoring the continuous monitoring assessments and reporting them as POA&Ms as needed. IRMD also implemented monthly POA&M/Audit finding review/status meetings to ensure continued progress towards closing findings.	Closed
3	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.	The FLRA takes the remediation of vulnerabilities seriously and has committed to NIST 800-53, Revision 4, RA-5. While all High vulnerabilities were remediated timely, the FLRA will work to improve on its remediation of medium classified vulnerabilities.	FY 2018
4	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.	The FLRA successfully implemented a new on and off boarding process, which address areas where interns were missed in the past.	Closed
5	On an annual basis, all FLRA employees should have their access reviewed to ensure it 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.	The FLRA expanded their review of user access to include office reviews. All offices are required to annually verify user access within specific offices.	Closed

Appendix 3
OIG Responses Report in Cyberscope

Inspector General

Section Report

2017
Annual FISMA Report

Federal Labor Relations Authority

Function 1: Identify - Risk Management

1 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 and PM-5; OMB M-04-25; NIST Cybersecurity Framework (CSF): ID.AM-1 – 4)?

Consistently Implemented (Level 3)

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)?

Managed and Measurable (Level 4)

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)?

Managed and Measurable (Level 4)

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; and FIPS 199)?

Consistently Implemented (Level 3)

5 To what extent has the organization established, communicated, and implemented its risk management policies, procedures, and strategy that include 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 800-39; NIST 800-53: PM-8, PM-9; CSF: ID RM-1 – ID.RM-3; OMB A-123; CFO Council ERM Playbook)?

Managed and Measurable (Level 4)

6 Has the organization defined an information security architecture and described how that architecture is integrated into and supports the organization's enterprise architecture to provide a disciplined and structured methodology for managing risk (NIST 800-39; FEA; NIST 800-53: PL-8, SA-3, and SA-8)?

Consistently Implemented (Level 3)

7 To what degree have roles and responsibilities of stakeholders involved in risk management, including the risk executive function/Chief Risk Officer, 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 800-39: Section 2.3.1 and 2.3.2; NIST 800-53: RA-1; CSF: ID.RM-1 – ID.GV-2, OMB A-123, CFO Council ERM Playbook)?

Managed and Measurable (Level 4)

Function 1: Identify - Risk Management

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)?

Optimized (Level 5)

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) selecting and implementing security controls to mitigate system-level risks (NIST 800--37; NIST 800-39; NIST 800--53: PL-2, RA-1; NIST 800-30; CSF:ID.RA-1 – 6)?

Defined (Level 2)

Comments: This Agency had vulnerability scans where the issues were not remediated timely, therefore this question was assessed as less than managed and measurable.

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)?

Managed and Measurable (Level 4)

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, 52.239-1; President's Management Council; NIST 800-53: SA-4; FedRAMP standard contract clauses; Cloud Computing Contract Best Practices; FY 2017 CIO FISMA Metrics: 1.7, 1.8)?

Managed and Measurable (Level 4)

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)?

Managed and Measurable (Level 4)

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

Managed and Measurable (Level 4)

Function 1: Identify - Risk Management

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?

There were issues with remediating vulnerability scans.

Calculated Maturity Level - Managed and Measurable (Level 4)

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; SP 800-128: Section 2.4)?

Managed and Measurable (Level 4)

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 location within an organization's SDLC; configuration monitoring; and applying configuration management requirements to contracted systems (NIST 800--128: Section 2.3.2; NIST 800--53: CM-9)?

Managed and Measurable (Level 4)

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 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, CM-8; FY 2017 CIO FISMA Metrics: 1.4, 1.5, and 2.1; 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 2017 CIO FISMA Metrics: 2.2; SANS/CIS Top 20 Security Controls 3.7)?

Managed and Measurable (Level 4)

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

Managed and Measurable (Level 4)

Function 2A: Protect - Configuration Management

20 To what extent has the organization adopted the Trusted Internet Connection (TIC) program to assist in protecting its network (FY 2017 CIO Metrics: 2.26, 2.27, 2.29; OMB M-08-05)?

Consistently Implemented (Level 3)

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 800-53: CM--2, CM-3)?

Managed and Measurable (Level 4)

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?

This Agency's systems are primarily COTS products, however there is a robust infrastructure in place for managing configuration changes.

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 800-53: AC-1, IA-1, PS-1; and the Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance (FICAM))?

Managed and Measurable (Level 4)

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

Managed and Measurable (Level 4)

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 27 through 31) (NIST 800-53: AC-1 and IA--1; Cybersecurity Strategy and Implementation Plan (CSIP); and SANS/CIS Top 20: 14.1)?

Managed and Measurable (Level 4)

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, PS- 3; and National Insider Threat Policy)?

Managed and Measurable (Level 4)

Function 2B: Protect - Identity and Access Management

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)

28 To what extent has the organization implemented strong authentication mechanisms (PIV or Level of Assurance 4 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; and Cybersecurity Sprint)?

Managed and Measurable (Level 4)

29 To what extent has the organization implemented strong authentication mechanisms (PIV or Level of Assurance 4 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; and Cybersecurity Sprint)?

Managed and Measurable (Level 4)

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 2017 CIO FISMA metrics: Section 2; NIST SP 800-53: AC-1, AC-2 (2), AC-17; CSIP)?

Managed and Measurable (Level 4)

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, SI-4; and FY 2017 CIO FISMA Metrics: Section 2)?

Managed and Measurable (Level 4)

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?

There were no issues this year as it relates to identity and access management.

Calculated Maturity Level - Managed and Measurable (Level 4)

Function 2C: Protect - Security Training

Function 2C: Protect - Security Training

33 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 800-53: AT-1; and NIST SP 800-50)?

Managed and Measurable (Level 4)

34 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 800-53: AT-2 and AT-3; NIST 800-50: Section 3.2; Federal Cybersecurity Workforce Assessment Act of 2015; National Cybersecurity Workforce Framework v1.0; NIST SP 800-181 (Draft); and CIS/SANS Top 20: 17.1)?

Managed and Measurable (Level 4)

35 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 800--53: AT-1; NIST 800-50: Section 3))

Managed and Measurable (Level 4)

36 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 questions 37 and 38 below) (NIST 800-53: AT-1 through AT-4; and NIST 800-50)

Managed and Measurable (Level 4)

37 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 800-53: AT-2; FY 17 CIO FISMA Metrics: 2.23; NIST 800-50: 6.2; SANS Top 20: 17.4)

Managed and Measurable (Level 4)

38 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 800-53: AT-3 and AT-4; FY 17 CIO FISMA Metrics: 2.23)?

Managed and Measurable (Level 4)

Function 2C: Protect - Security Training

39.1 Please provide the assessed maturity level for the agency's Protect - Configuration Management/Identity and Access Management/Security Training (Functions 2A - 2C).

Managed and Measurable (Level 4)

39.2 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?

There were no issues for security training this year.

Calculated Maturity Level - Managed and Measurable (Level 4)

Function 3: Detect - ISCM

40 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)

41 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; collecting 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 43)

Managed and Measurable (Level 4)

42 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 2017 CIO FISMA Metrics)?

Managed and Measurable (Level 4)

43 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)

44 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)

Function 3: Detect - ISCM

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

Managed and Measurable (Level 4)

45.2 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?

There were no issues with Continuous Monitoring this year.

Calculated Maturity Level - Managed and Measurable (Level 4)

Function 4: Respond - Incident Response

46 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 800-61 Rev. 2; FY 2017 CIO FISMA Metrics: 4.1, 4.3, and 4.6)? (Note: The overall maturity level should take into consideration the maturity of questions 48 - -52)

Managed and Measurable (Level 4)

47 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; NIST SP 800-83; NIST SP 800-61 Rev. 2; OMB M-16-03; OMB M-16-04; FY 2017 CIO FISMA Metrics: 1.6 and 4.5; and US-CERT Federal Incident Notification Guidelines)?

Managed and Measurable (Level 4)

48 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; US- CERT Incident Response Guidelines)?

Managed and Measurable (Level 4)

49 How mature are the organization's processes for incident handling (NIST 800-53: IR-4)?

Managed and Measurable (Level 4)

50 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-16-03; NIST 800-53: IR-6; US-CERT Incident Notification Guidelines)?

Managed and Measurable (Level 4)

51 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 and enter into contracts, as appropriate, for incident response support (FY 2017 CIO FISMA Metrics: 4.4; NIST SP 800-86)?

Consistently Implemented (Level 3)

Function 4: Respond - Incident Response

52 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)

Managed and Measurable (Level 4)

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

Managed and Measurable (Level 4)

53.2 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?

There were no issues with Incident Response this year.

Calculated Maturity Level - Managed and Measurable (Level 4)

Function 5: Recover - Contingency Planning

54 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 800-53: CP-1 and CP-2; NIST 800-34; NIST 800-84; FCD-1: Annex B)?

Managed and Measurable (Level 4)

55 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 56-60) (NIST SP 800-34; NIST SP 800--161).

Managed and Measurable (Level 4)

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

Consistently Implemented (Level 3)

Function 5: Recover - Contingency Planning

57 To what extent does the organization ensure that information system contingency plans are developed, maintained, and integrated with other continuity plans (NIST 800-53: CP-2; NIST 800-34)?

Managed and Measurable (Level 4)

58 To what extent does the organization perform tests/exercises of its information system contingency planning processes (NIST 800-34; NIST 800-53: CP-3, CP-4)?

Managed and Measurable (Level 4)

59 To what extent does the organization perform information system backup and storage, including use of alternate storage and processing sites, as appropriate (NIST 800--53: CP-6, CP-7, CP-8, and CP-9; NIST SP 800-34: 3.4.1, 3.4.2, 3.4.3; FCD1; NIST CSF: PR.IP- 4; and NARA guidance on information systems security records)?

Consistently Implemented (Level 3)

60 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 800-53: CP-2, IR-4)?

Managed and Measurable (Level 4)

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

Managed and Measurable (Level 4)

61.2 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?

There were no issues with contingency planning this year.

Calculated Maturity Level - Managed and Measurable (Level 4)

Function 0: Overall

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

Effective

Function 0: Overall

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.

Overall, this Agency was extremely successful in deploying IT controls. There were no new issues. Of the prior year issues, only one was open, which involved the timely remediation of vulnerabilities.

APPENDIX A: Maturity Model Scoring

Function 1: Identify - Risk Management

Function	Count
Ad-Hoc	0
Defined	1
Consistently Implemented	3
Managed and Measurable	7
Optimized	1
Function Rating: Managed and Measurable (Level 4)	0

Function 2A: Protect - Configuration Management

Function	Count
Ad-Hoc	0
Defined	0
Consistently Implemented	1
Managed and Measurable	7
Optimized	0
Function Rating: Managed and Measurable (Level 4)	0

Function 2B: Protect - Identity and Access Management

Function	Count
Ad-Hoc	0
Defined	0
Consistently Implemented	1
Managed and Measurable	8
Optimized	0
Function Rating: Managed and Measurable (Level 4)	0

Function 2C: Protect - Security Training

Function	Count
Ad-Hoc	0
Defined	0
Consistently Implemented	0
Managed and Measurable	6
Optimized	0
Function Rating: Managed and Measurable (Level 4)	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)	0

Function 4: Respond - Incident Response

Function	Count
Ad-Hoc	0
Defined	0
Consistently Implemented	1
Managed and Measurable	6
Optimized	0
Function Rating: Managed and Measurable (Level 4)	0

Function 5: Recover - Contingency Planning

Function	Count
Ad-Hoc	0
Defined	0
Consistently Implemented	2
Managed and Measurable	5
Optimized	0
Function Rating: Managed and Measurable (Level 4)	0

Maturity Levels by Function

Function	Calculated Maturity Level	Assessed Maturity Level	Explanation
Function 1: Identify - Risk Management	Managed and Measurable (Level 4)	Managed and Measurable (Level 4)	
Function 2: Protect - Configuration Management / Identity Management / 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	Managed and Measurable (Level 4)	Managed and Measurable (Level 4)	
Function 5: Recover - Contingency Planning	Managed and Measurable (Level 4)	Managed and Measurable (Level 4)	
Overall	Effective	Effective	

Appendix 4
Report Distribution

Federal Labor Relations Authority

Ernest DuBester, Member
Michael Jeffries, Acting Executive Director
Fred Jacob, Solictor

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