



Office of Inspector General

Evaluation of FLRA's Compliance
with the FISMA FY 2021

EVALUATION OF THE
FEDERAL LABOR RELATIONS
AUTHORITY COMPLIANCE
WITH THE FEDERAL
INFORMATION SECURITY
MANAGEMENT ACT
FISCAL YEAR 2021

Report No. MAR-22-01
October 2021

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	5
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
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
SP	NIST Special Publication Series

Evaluation of FLRA's Compliance with the FISMA FY 2021

Report No. MAR-22-01

October 25, 2021

The Honorable Ernest DeBester
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) 2021 report to the Office of Management and Budget (OMB) and Congress.

Results in Brief

During our FY 2021 evaluation, we noted that FLRA has taken significant steps to improve the information security program. We also noted that FLRA does take information security weaknesses seriously. This year's testing identified no new findings. We followed up on the five prior year recommendations and closed four.

Background

On December 17, 2002, the President signed into law H.R. 2458, the E-Government Act of 2002 (Public Law 107-347). Title III of the E-Government Act of 2002, commonly referred to as FISMA, focuses on improving oversight of Federal information security programs and facilitating progress in correcting agency information security weaknesses. FISMA requires Federal agencies to develop, document, and implement an agency-wide information security program that provides security for the information and information systems that support the operations and assets of the agency. This program includes providing security for information systems provided or managed by another agency, contractor, or other source. FISMA assigns specific responsibilities to agency heads and Inspectors General (IGs). It is supported by security policy promulgated through OMB, and risk-based standards and guidelines published in the National Institute of Standards and Technology (NIST) Special Publication (SP) series.

Under FISMA, agency heads are responsible for providing information security protections commensurate with the risk and magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems. FISMA directs Federal agencies to report annually to the OMB Director, Comptroller General, and selected congressional

committees on the adequacy and effectiveness of agency information security policies, procedures, and practices and compliance with FISMA. In addition, FISMA requires agencies to have an annual independent evaluation performed of their information security programs and practices and to report the evaluation results to OMB. FISMA states that the independent evaluation is to be performed by the agency IG or an independent external auditor as determined by the IG. Implementing adequate information security controls is essential to ensuring an organization can effectively meet its mission. The IG plays an essential role in supporting Federal agencies in identifying areas for improvement. In support of that critical goal the FLRA supports the development of a strategy to secure the FLRA computing environment which centers on providing confidentiality, integrity, and availability.

Scope and Methodology

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



Dembo Jones, P.C.

North Bethesda, Maryland
October 25, 2021

Appendix 1

Prior Year Recommendations

1. **(Partially Closed)** FLRA should develop, review and update, as necessary, the following information security program policies and procedures in accordance with NIST and agency requirements:
 - a. Risk policies and procedures.
 - b. System and Services Acquisition Policy
 - c. Personnel Security policy.
 - d. Security Assessment policy.
 - e. Configuration Management policy.
 - f. Configuration Management Plan.
 - g. Incident Response policy.
 - h. Security Awareness policy.
 - i. Identification and Authentication policy.
 - j. Access policy.
 - k. Mobile Code Usage and Restrictions Policy

Deficiency	
Risk policy and procedures have not been formalized, reviewed and approved.	Closed
Update the Acquisition policy to ensure that it contains stipulations that require external service providers meet or exceed the NIST security requirements.	Open
FLRA's Personnel Security policy and procedures have not been formalized, reviewed and approved..	Closed
FLRA's Security Assessment policy and procedures formalized, reviewed and approved.	Closed
The Configuration Management Plan and policy has not been formalized, reviewed and approved.	Open
The Incident Response policy has not been formalized, reviewed and approved.	Closed
The Security Awareness policy has not been formalized, reviewed and approved.	Closed
The Identification and Authentication policy has not been formalized, reviewed and approved.	Closed
The Access Control Policy has not been formalized, reviewed and approved.	Closed
Mobile code technologies and usage restrictions have not been formally documented in a Policy.	Open

2. **(Closed)** All vulnerabilities should be reviewed in terms of their risk classification (e.g. high, medium, and low). Furthermore, IT should establish a formalized policy for how timely deficiencies (high, medium, and low) need to be remediated. Best practices across other agencies remediate high vulnerabilities within 1 business day and medium vulnerabilities within 3-5 business days, therefore, FLRA should follow best practices.
3. **(Closed)** Ensure all staff (employees and contractors) are assigned a risk classification for each position so that audit monitoring can be focused on areas of concern.
4. **(Closed)** On an annual basis, all FLRA employees should have their access reviewed (by the respective employee's immediate supervisor) to ensure it is still commensurate with their job functions.
5. **(Closed)** On a semi-annual basis, all admin users' accounts should be reviewed to ensure their authorizations are still appropriate.




UNITED STATES OF AMERICA
FEDERAL LABOR RELATIONS AUTHORITY

October 22, 2021

MEMORANDUM

TO: Dana Rooney
Inspector General

FROM: Michael Jeffries 
Executive Director

SUBJECT: Management Response to FY2021 Draft Report on the FLRA's Compliance with the Federal Information Security Management Act

Thank you for the opportunity to review and provide comments on the Office of Inspector General's (OIG) draft Management Advisory Review report "*Evaluation of FLRA's Compliance with the FISMA FY 2021.*" The Federal Labor Relations Authority (FLRA) appreciates the very in-depth review of our information security program, and we are overjoyed that, out of the 900+ controls for which we are responsible, there were *no new findings* in this year's report.

We are also extremely proud to see that our actions throughout the course of this year have resulted in the complete closure of 4 of the 5 recommendations from the FY 2020 review. The remaining recommendation consisted of 12 policy documents that FLRA either did not have in effect, or that were not in full compliance with all current regulations. This year's report reflects the fact that over 100 pages of new policy and procedure documents were authored, ratified, and implemented throughout the course of this year.

RECOMMENDATIONS FOR FINDING NO. 01 – POLICIES AND PROCEDURES

1. *Update the Acquisition policy to ensure that it contains stipulations that require external service providers meet or exceed the NIST security requirements.*

Management Response: The Executive Director concurs with the recommendation and will work with the Director of the Information Resources Management Division (IRMD) and the Director of the Administrative Services Division (ASD) to ensure that the Acquisition Policy document is updated, thoroughly reviewed, and enacted timely.

2. *The Configuration Management Plan and policy has not been formalized, reviewed and approved.*

Management Response: This past year, the FLRA Configuration Management Plan and

procedures were created, but the *policy* document was not ratified. The Executive Director concurs with the recommendation and will work with the Director of IRMD to ensure that Configuration Management Policy document is authored, ratified, and implemented.

3. *Mobile code technologies and usage restrictions have not been formally documented in a Policy.*

Management Response: The Executive Director concurs with the recommendations and will work with the Director of IRMD to ensure that all documents are created, thoroughly reviewed, and enacted timely.

We appreciate your consideration of these responses in finalizing the report and look forward to continuing our efforts to find innovative ways to improve.

We would like to thank the OIG for your efforts and continued collaboration in support of FLRA programs.

Appendix 3
OIG Responses Report in Cyberscope

Inspector General

Section Report

2021

IG Annual

Federal Labor Relations Authority

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.

This year's FISMA assessment included an array of controls testing. The controls selected were from NIST 800-53 (Rev. 4 and 5) and mapped to the Cyberscope questions. The agency (FLRA) has made numerous strides this year, as a large number of prior year findings were closed in the current year. Although the FLRA is a small agency as compared to the larger agencies (e.g. CFO Act agencies), and has a small IT staff; the agency is quite effective in deploying IT controls throughout the agency.

Function 1A: 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. Rev. 4: CA-3, PM-5, and CM-8; NIST Cybersecurity Framework (CSF): ID.AM-1 - 4; FY 2021 CIO FISMA Metrics: 1.1, 1.1.5 and 1.4, OMB A-130, NIST SP 800-37, Rev. 2: Task P-18).

Optimized (Level 5)

2. To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets (including GFE and Bring Your Own Device (BYOD) mobile devices) connected to the organization's network with the detailed information necessary for tracking and reporting (NIST SP 800-53 Rev. 4: CA-7 and CM-8; NIST SP 800-137; NIST IR 8011; Federal Enterprise Architecture (FEA) Framework, v2; FY 2021 CIO FISMA Metrics: 1.2, 1.3, 2.2, 3.9, CSF: ID.AM-1; NIST SP 800-37, Rev. 2: Task P-10).

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 Rev. 4: CA-7, CM-8, and CM-10; NIST SP 800-137; NIST IR 8011; FEA Framework, v2; FY 2021 CIO FISMA Metrics: 1.2.5, 1.3.3, 1.3.9, 1.3.10, 3.10; CSF: ID.AM-2; NIST SP 800-37, Rev. 2: Task P-10)?

Managed and Measurable (Level 4)

Function 1A: Identify - Risk Management

4. To what extent has the organization categorized and communicated the importance/priority of information systems in enabling its missions and business functions, including for high value assets (NIST SP 800-53 Rev. 4: RA-2, PM-7, and PM-11; NIST SP 800-60; NIST SP 800-37 (Rev. 2); CSF: ID.BE-3, ID.AM-5, and ID.SC-2; FIPS 199; FY 2021 CIO FISMA Metrics: 1.1; OMB M-19-03; NIST SP 800-37, Rev. 2: Task C-2, C-3, P-4, P-12, P-13, S-1 - S-3, NIST IR 8170)?

Consistently Implemented (Level 3)

Comments: High-value assets are not being tracked at this time.

5. To what extent does the organization ensure that information system security risks are adequately managed at the organizational, mission/business process, and information system levels (NIST SP 800-39; NIST SP 800-53 Rev. 4: RA-3, PM-9; NIST IR 8286, CSF: ID.RM-1 - ID.RM-3; OMB A-123; OMB M-16-17; OMB M-17-25; NIST SP 800-37 (Rev. 2): Tasks P-2, P-3, P-14, R-2, and R-3)?

Managed and Measurable (Level 4)

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 (Federal Information Technology Acquisition Reform Act (FITARA), NIST SP 800-39; NIST SP 800-160; NIST SP 800-37 (Rev. 2) Task P-16; OMB M-19-03; OMB M-15-14, FEA Framework; NIST SP 800-53 Rev. 4: PL-8, SA-3, SA-8, SA-9, SA-12, and PM-9; NIST SP 800-163, Rev. 1 CSF: ID.SC-1 and PR.IP-2; SECURE Technology Act: s. 1326)?

Consistently Implemented (Level 3)

Comments: The agency has not implemented Supply Chain Risk Management procedures at this time.

7. To what extent have the roles and responsibilities of internal and external stakeholders involved in cybersecurity risk management processes been defined, communicated, and implemented across the organization (NIST SP 800-39: Section 2.3.1, 2.3.2, and Appendix D; NIST SP 800-53 Rev. 4: RA-1; CSF: ID.AM-6, ID.RM-1, and ID.GV-2; NIST IR 8286, Section 3.1.1, OMB A-123; NIST SP 800-37 (Rev. 2) Section 2.8 and Task P-1; OMB M-19-03)?

Managed and Measurable (Level 4)

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 Rev. 4: CA-5; NIST SP 800-37 (Rev. 2) Task A-6, R-3; OMB M-04-14, M-19-03, CSF v1.1, ID.RA-6)?

Managed and Measurable (Level 4)

9. To what extent does the organization ensure that information about cybersecurity risks is communicated in a timely and effective manner to appropriate internal and external stakeholders (OMB A-123; OMB Circular A-11 and OMB M-19-03; CSF: Section 3.3; NIST SP 800-37 (Rev. 2) Task M-5; SECURE Technology Act: s. 1326, NIST IR 8170 and 8286)?

Managed and Measurable (Level 4)

Function 1A: Identify - Risk Management

10. To what extent does the organization utilize technology/ automation to provide a centralized, enterprise wide (portfolio) view of cybersecurity risk management activities across the organization, including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards (NIST SP 800-39; OMB A-123 and NIST IR 8286)?

Consistently Implemented (Level 3)

Comments: There is no automation for this question at this time.

- 11.1. Please provide the assessed maturity level for the agency's Identify - Risk Management program.

Managed and Measurable (Level 4)

- 11.2. 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?

FLRA has made great strides this year in complying with FISMA, as evidenced by this year's resolution of the various prior year findings. Please refer to the Annual FISMA report.

Function 1B: Identify - Supply Chain Risk Management

12. To what extent does the organization utilize an organization wide SCRM strategy to manage the supply chain risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services? (The Federal Acquisition Supply Chain Security Act of 2018 (H.R. 7327, 41 USC Chap. 13 Sub chap. III and Chap. 47, P.L. 115-390) (Dec. 21, 2018), NIST SP 800-53, Rev. 5, PM-30, NIST IR 8276)?

Consistently Implemented (Level 3)

Comments: FLRA has only recently started to develop Supply Chain Risk Management policies and procedures and hopes to have this completed and ready for assessment in the next audit year.

13. To what extent does the organization utilize SCRM policies and procedures to manage SCRM activities at all organizational tiers (The Federal Acquisition Supply Chain Security Act of 2018, NIST 800-53, Rev. 5, SR-1, NIST CSF v1.1, ID.SC-1 and ID.SC-5, NIST IR 8276)?

Ad Hoc (Level 1)

Comments: FLRA has only recently started to develop Supply Chain Risk Management policies and procedures and hopes to have this completed and ready for assessment in the next audit year.

14. To what extent does the organization ensure that products, system components, systems, and services of external providers are consistent with the organization's cybersecurity and supply chain requirements. (The Federal Acquisition Supply Chain Security Act of 2018, NIST SP 800-53 REV. 5: SA-4, SR-3, SR-5, SR-6 (as appropriate); NIST SP 800-152; FedRAMP standard contract

Function 1B: Identify - Supply Chain Risk Management

clauses; Cloud Computing Contract Best Practices; OMB M-19-03; OMB A-130; CSF: ID.SC-2 through 4, NIST IR 8276).

Ad Hoc (Level 1)

Comments: FLRA has only recently started to develop Supply Chain Risk Management policies and procedures and hopes to have this completed and ready for assessment in the next audit year.

15. To what extent does the organization ensure that counterfeit components are detected and prevented from entering the organization's systems? (800-53 rev 5 SR-11, 11 (1), and 11(2))

Ad Hoc (Level 1)

Comments: FLRA has only recently started to develop Supply Chain Risk Management policies and procedures and hopes to have this completed and ready for assessment in the next audit year.

- 16.1. Please provide the assessed maturity level for the agency's Identify - Supply Chain Risk Management program.

Ad Hoc (Level 1)

- 16.2. Please provide the assessed maturity level for the agency's Identify Function.

Ad Hoc (Level 1)

- 16.3. Provide any additional information on the effectiveness (positive or negative) of the organization's Supply Chain 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?

Supply Chain Risk Management has not been deployed for this agency at this time. The agency (FLRA) has recently commenced the development of SCRM policies and procedures.

Function 2A: Protect - Configuration Management

17. To what extent have the roles and responsibilities of configuration management stakeholders been defined, communicated, and implemented across the agency, and appropriately resourced (NIST SP 800-53 REV. 4: CM-1; NIST SP 800-128: Section 2.4)?

Ad Hoc (Level 1)

Comments: The FLRA had a deficiency related to a lack of a Configuration Management Plan (CMP).

18. 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 REV. 4: CM-9)?

Ad Hoc (Level 1)

Function 2A: Protect - Configuration Management

Comments: The FLRA had a deficiency related to a lack of a Configuration Management Plan (CMP).

19. 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 REV. 4: CM-2 and CM-8; FY 2021 CIO FISMA Metrics: 2.2, 3.9.2, and 3.10.1; CSF: DE.CM-7 and PR.IP-1)?

Consistently Implemented (Level 3)

Comments: There is currently no automation to address this question at the Managed and Measurable level.

20. To what extent does the organization utilize configuration settings/common secure configurations for its information systems? (NIST SP 800-53 REV. 4: CM-6, CM-7, RA-5, and SI-2; NIST SP 800-70, Rev. 4, FY 2021 CIO FISMA Metrics: 2.1, 2.2, 4.3; SANS/CIS Top 20 Security Controls 3.7; CSF: ID.RA-1 and DE.CM-8)?

Consistently Implemented (Level 3)

Comments: There is currently no automation to address this question at the Managed and Measurable level.

21. To what extent does the organization utilize flaw remediation processes, including patch management, to manage software vulnerabilities (NIST SP 800-53 REV. 4: CM-3, RA-5, SI-2, and SI-3; NIST SP 800-40, Rev. 3; SANS/CIS Top 20, Control 4.5; FY 2021 CIO FISMA Metrics: 1.3.7, 1.3.8, 2.13, 2.14; CSF: ID.RA-1; DHS Binding Operational Directives (BOD) 18-02 and 19-02)?

Consistently Implemented (Level 3)

Comments: There is currently no automation to address this question at the Managed and Measurable level.

22. To what extent has the organization adopted the Trusted Internet Connection (TIC) program to assist in protecting its network (OMB M-19-26, DHS-CISA TIC 3.0 Core Guidance Documents)

Managed and Measurable (Level 4)

23. 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 REV. 4: CM-2, CM-3 and CM-4; CSF: PR.IP-3).

Consistently Implemented (Level 3)

Comments: Qualitative and quantitative measures are not being performed at this time.

24. To what extent does the organization utilize a vulnerability disclosure policy (VDP) as part of its vulnerability management program for internet-accessible federal systems (OMB M-20-32 and DHS BOD 20-01)?

Ad Hoc (Level 1)

Comments: The FLRA doesn't have a VDP at this time.

Function 2A: Protect - Configuration Management

25.1. Please provide the assessed maturity level for the agency's Protect - Configuration Management program.

Consistently Implemented (Level 3)

25.2. 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?

FLRA has made great strides this year in complying with FISMA, as evidenced by this year's resolution of the various prior year findings. Please refer to the Annual FISMA report.

Function 2B: Protect - Identity and Access Management

26. To what extent have the roles and responsibilities of identity, credential, and access management (ICAM) stakeholders been defined, communicated, and implemented across the agency, and appropriately resourced (NIST SP 800-53 REV. 4: AC-1, IA-1, and PS-1; NIST SP 800-63-3 and 800-63A, B, and C; Federal Identity, Credential, and Access Management (FICAM) playbooks and guidance (see idmanagement.gov), OMB M-19-17)?

Managed and Measurable (Level 4)

27. To what extent does the organization utilize a comprehensive ICAM policy, strategy, process, and technology solution roadmap to guide its ICAM processes and activities (FICAM, OMB M-19-17; NIST SP 800-53 REV. 4: AC-1 and IA-1; OMB M-19-17; SANS/CIS Top 20: 14.1; DHS ED 19-01; CSF: PR.AC-4 and 5)?

Consistently Implemented (Level 3)

Comments: There are no automated mechanisms at this time.

28. To what extent has the organization developed and implemented processes for assigning position risk designations and performing appropriate personnel screening prior to granting access to its systems (NIST SP 800-53 REV. 4: PS-2 and PS-3; National Insider Threat Policy; CSF: PR.IP-11, OMB M-19-17)?

Consistently Implemented (Level 3)

Comments: There are no automated mechanisms at this time.

29. 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 REV. 4: AC-8, PL-4, and PS-6)?

Consistently Implemented (Level 3)

Comments: There are no automated mechanisms at this time.

30. To what extent has the organization implemented strong authentication mechanisms (PIV or an Identity Assurance Level

Function 2B: Protect - Identity and Access Management

(IAL)3/Authenticator Assurance Level (AAL) 3 credential) for non-privileged users to access the organization's facilities [organization-defined entry/exit points], networks, and systems, including for remote access (HSPD-12; NIST SP 800-53 REV. 4: AC-17, IA-2, IA-5, IA-8, and PE-3; NIST SP 800-128; FIPS 201-2; NIST SP 800-63, 800-157; FY 2021 CIO FISMA Metrics: 2.4, 2.7, CSF: PR.AC-1 and 6; OMB M-19-17, and NIST SP 800-157)?

Managed and Measurable (Level 4)

31. To what extent has the organization implemented strong authentication mechanisms (PIV or an Identity Assurance Level (IAL)3/Authenticator Assurance Level (AAL) 3 credential) for privileged users to access the organization's facilities [organization-defined entry/exit points], networks, and systems, including for remote access (HSPD-12; NIST SP 800-53 REV. 4: AC-17, PE-3; NIST SP 800-128; FIPS 201-2; NIST SP 800-63 and 800-157; OMB M-19-17, FY 2021 CIO FISMA Metrics: 2.3, 2.5, and 2.7; CSF: PR.AC-1 and 6; and DHS ED 19-01)?

Managed and Measurable (Level 4)

32. 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 2021 CIO FISMA Metrics: 2.3, 2.5, 2.6, and 2.7; OMB M-19-17, NIST SP 800-53 REV. 4: AC-1, AC-2, AC-5, AC-6, AC-17; AU-2, AU-3, AU-6, and IA-4; DHS ED 19-01; CSF: PR.AC-4).

Consistently Implemented (Level 3)

Comments: There are no automated mechanisms at this time.

33. 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 REV. 4: AC-11, AC-12, AC-17, AC-19, AU-2, IA-7, SC-10, SC-13, and SI-4; CSF: PR.AC-3; and FY 2021 CIO FISMA Metrics: 2.10 and 2.11).

Managed and Measurable (Level 4)

- 34.1. Please provide the assessed maturity level for the agency's Protect - Identity and Access Management program.

Managed and Measurable (Level 4)

- 34.2. 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?

FLRA has made great strides this year in complying with FISMA, as evidenced by this year's resolution of the various prior year findings. Please refer to the Annual FISMA report.

Function 2C: Protect - Data Protection and Privacy

35. 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; NIST SP 800-37 (Rev. 2) Section 2.3, Task P-1 ; OMB M-20-04; OMB M-19-03; OMB A-130, Appendix I; CSF: ID.GV-3; NIST SP 800-53 REV. 4: AR-4 and Appendix J, FY 2020 SAOP FISMA metrics, Sections 1 through 4, 5(b), NIST Privacy Framework)?

Managed and Measurable (Level 4)

36. 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 REV. 4; Appendix J, SC-8, SC-28, MP-3, and MP-6; NIST SP 800-37 (Rev. 2); FY 2021 CIO FISMA Metrics: 2.8, 2.12; DHS BOD 18-02; CSF: PR.DS-1, PR.DS-2, PR.PT-2, and PR.IP-6)?

- 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)

37. To what extent has the organization implemented security controls to prevent data exfiltration and enhance network defenses? (NIST SP 800-53 REV. 4: SI-3, SI-7(8), SI-4(4) and (18), SC-7(10), and SC-18; FY 2021 CIO FISMA Metrics: 3.8; DHS BOD 18-01; DHS ED 19-01; CSF: PR.DS-5)?

Consistently Implemented (Level 3)

Comments: There is currently no qualitative and quantitative measurements at this time.

38. 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 REV. 4: Appendix J, SE-2; FY 2020 SAOP FISMA metrics, Section 12; OMB M-17-12; and OMB M-17-25)?

Consistently Implemented (Level 3)

Comments: There is currently no qualitative and quantitative measurements at this time.

39. To what extent does the organization ensure that privacy awareness training is provided to all individuals, including role-based privacy training (NIST SP 800-53 REV. 4: AR-5, FY 2020 SAOP FISMA Metrics, Sections 9 10, and 11)?

Managed and Measurable (Level 4)

- 40.1. Please provide the assessed maturity level for the agency's Protect - Data Protection and Privacy program.

Managed and Measurable (Level 4)

- 40.2. 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

Function 2C: Protect - Data Protection and Privacy

questions above and based on all testing performed, is the data protection and privacy program effective?

FLRA has made great strides this year in complying with FISMA, as evidenced by this year's resolution of the various prior year findings. Please refer to the Annual FISMA report.

Function 2D: Protect - Security Training

41. To what extent have the roles and responsibilities of security awareness and training program stakeholders been defined, communicated, and implemented 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 REV. 4: AT-1; and NIST SP 800-50).

Consistently Implemented (Level 3)

Comments: FLRA IT operations were only able to meet the requirements at the "Consistently Implemented" level.

42. 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 REV. 4: 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)?

Managed and Measurable (Level 4)

43. To what extent does the organization utilize a security awareness and training strategy/plan that leverages its skills assessment and is adapted to its mission and risk environment? (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 REV. 4: AT-1; NIST SP 800-50: Section 3; CSF: PR.AT-1).

Consistently Implemented (Level 3)

Comments: Qualitative and quantitative measurements were not in place at this time.

44. To what extent does the organization ensure that security awareness training is provided to all system users and is tailored based on its mission, risk environment, 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 REV. 4: AT-1, AT-2; FY 2021 CIO FISMA Metrics: 2.15; NIST SP 800-50: 6.2; CSF: PR.AT-2; SANS Top 20: 17.4).

Managed and Measurable (Level 4)

Function 2D: Protect - Security Training

45. To what extent does the organization ensure that specialized security training is provided to individuals with significant security responsibilities (as defined in the organization's security policies and procedures and in accordance with 5 Code of Federal Regulation 930.301) (NIST SP 800-53 REV. 4: AT-3 and AT-4; FY 2021 CIO FISMA Metrics: 2.15, and 5 Code of Federal Regulation 930.301)?

Managed and Measurable (Level 4)

- 46.1. Please provide the assessed maturity level for the agency's Protect - Security Training program.

Managed and Measurable (Level 4)

- 46.2. Please provide the assessed maturity level for the agency's Protect function.

Managed and Measurable (Level 4)

- 46.3. 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?

FLRA has made great strides this year in complying with FISMA, as evidenced by this year's resolution of the various prior year findings. Please refer to the Annual FISMA report.

Function 3: Detect - ISCM

47. To what extent does the organization utilize information security continuous monitoring (ISCM) policies and an ISCM strategy that addresses ISCM requirements and activities at each organizational tier (NIST SP 800-37 (Rev. 2) Task P-7; NIST SP 800-137: Sections 3.1 and 3.6)?

Managed and Measurable (Level 4)

48. To what extent have ISCM stakeholders and their roles, responsibilities, levels of authority, and dependencies been defined, communicated, and implemented across the organization (NIST SP 800-53 REV. 4: CA-1; NIST SP 800-137; CSF: DE.DP-1; NIST 800-37, Rev. 2 Task P-7 and S-5)

Managed and Measurable (Level 4)

49. How mature are the organization's processes for performing ongoing information system assessments, granting system authorizations, including developing and maintaining system security plans, and monitoring system security controls (OMB A-130, NIST SP 800-137: Section 2.2; NIST SP 800-53 REV. 4: CA-2, CA-6, and CA-7; NIST Supplemental Guidance on Ongoing Authorization; NIST SP 800-37 (Rev. 2) Task S-5; NIST SP 800-18, Rev. 1, NIST IR 8011; OMB M-14-03; OMB M-19-03)

Managed and Measurable (Level 4)

Function 3: Detect - ISCM

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 domain/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?

This section had "Managed and Measurable" for all questions, therefore there are no additional comments at this time.

Function 4: Respond - Incident Response

52. To what extent does the organization utilize an incident response plan to provide a formal, focused, and coordinated approach to responding to incidents (NIST SP 800-53 REV. 4: IR-8; NIST SP 800-61 Rev. 2, section 2.3.2; CSF, RS.RP-1, Presidential Policy Directive (PPD) 8 - National Preparedness)?

Consistently Implemented (Level 3)

Comments: There were no qualitative and quantitative measurements at this time.

53. To what extent have incident response team structures/models, stakeholders, and their roles, responsibilities, levels of authority, and dependencies been defined, communicated, and implemented across the organization (NIST SP 800-53 REV. 4: IR-7; NIST SP 800-83; NIST SP 800-61 Rev. 2; CSF, RS.CO-1, OMB M-20-04; FY 2021 CIO FISMA Metrics: Section 4; CSF: RS.CO-1; and US-CERT Federal Incident Notification Guidelines)?

Managed and Measurable (Level 4)

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-20-04; CSF: DE.AE-1, DE.AE-2 -5, PR.DS-6, RS.AN-1 and 4, and PR.DS-8; and US-CERT Incident Response Guidelines)

Consistently Implemented (Level 3)

Comments: There were no qualitative and quantitative measurements at this time.

55. How mature are the organization's processes for incident handling (NIST 800-53: IR-4; NIST SP 800-61, Rev. 2; CSF: RS.MI-1 and 2)

Consistently Implemented (Level 3)

Function 4: Respond - Incident Response

Comments: There were no qualitative and quantitative measurements at this time.

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-20-04; NIST SP 800-53 REV. 4: IR-6; US-CERT Incident Notification Guidelines; PPD-41; CSF: RS.CO-2 through 5; DHS Cyber Incident Reporting Unified Message)

Consistently Implemented (Level 3)

Comments: The FLRA did not meet the stipulations at the "Managed and Measurable" at this time (for this question).

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 (NIST SP 800-86; NIST SP 800-53 REV. 4: IR-4; OMB M-20-04; PPD-41).

Managed and Measurable (Level 4)

58. To what extent 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)

Managed and Measurable (Level 4)

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

Consistently Implemented (Level 3)

- 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?

FLRA has made great strides this year in complying with FISMA, as evidenced by this year's resolution of the various prior year findings. Please refer to the Annual FISMA report.

Function 5: Recover - Contingency Planning

60. To what extent have roles and responsibilities of stakeholders involved in information systems contingency planning been defined, communicated, and implemented across the organization, including appropriate delegations of authority (NIST SP 800-53 REV. 4: CP-1, CP-2, and CP-3; NIST SP 800-34; NIST SP 800-84; FCD-1: Annex B)?

Function 5: Recover - Contingency Planning

Managed and Measurable (Level 4)

61. To what extent does the organization ensure that the results of business impact analyses (BIA) are used to guide contingency planning efforts (NIST SP 800-53 REV. 4: CP-2; NIST SP 800-34, Rev. 1, 3.2; NIST IR 8286; FIPS 199; FCD-1; OMB M-19-03; FY 2021 CIO FISMA Metrics, Section 5; CSF:ID.RA-4)?

Consistently Implemented (Level 3)

Comments: A BIA was not present this year, therefore this remained at the "Consistently Implemented" level.

62. 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 REV. 4: CP-2; NIST SP 800-34; FY 2021 CIO FISMA Metrics: 5.1; OMB M-19-03; CSF: PR.IP-9)?

Consistently Implemented (Level 3)

Comments: The FLRA was not able to meet the objectives at the "Managed and Measurable" level. The highest objectives met were at the "Consistently Implemented" level.

63. To what extent does the organization perform tests/exercises of its information system contingency planning processes (NIST SP 800-34; NIST SP 800-53 REV. 4: CP-3 and CP-4; FY 2021 CIO FISMA Metrics, Section 5; CSF: ID.SC-5 and CSF: PR.IP-10)?

Consistently Implemented (Level 3)

Comments: There were no automated mechanisms deployed at this time.

64. 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 REV. 4: 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 2021 CIO FISMA Metrics, Section 5; and NARA guidance on information systems security records)?

Consistently Implemented (Level 3)

Comments: Supply Chain controls were not assessed this year.

65. 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 REV. 4: CP-2 and IR-4)?

Managed and Measurable (Level 4)

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

Consistently Implemented (Level 3)

- 66.2. 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

Function 5: Recover - Contingency Planning

questions above and based on all testing performed, is the contingency program effective?

FLRA has made great strides this year in complying with FISMA, as evidenced by this year's resolution of the various prior year findings. Please refer to the Annual FISMA report.

APPENDIX A: Maturity Model Scoring

A.1. Please provide the assessed maturity level for the agency's Overall status.

Function 1A: Identify - Risk Management

Function	Count
Ad-Hoc	0
Defined	0
Consistently Implemented	3
Managed and Measurable	6
Optimized	1
<hr/>	
Calculated Rating: Managed and Measurable (Level 4)	
Assessed Rating: Managed and Measurable (Level 4)	

Function 1B: Identify - Supply Chain Risk Management

Function	Count
Ad-Hoc	3
Defined	0
Consistently Implemented	1
Managed and Measurable	0
Optimized	0
<hr/>	
Calculated Rating: Ad Hoc (Level 1)	
Assessed Rating: Ad Hoc (Level 1)	

Function 2A: Protect - Configuration Management

Function	Count
Ad-Hoc	3

APPENDIX A: Maturity Model Scoring

Defined	0
Consistently Implemented	4
Managed and Measurable	1
Optimized	0
<hr/>	
Calculated Rating: Consistently Implemented (Level 3)	
Assessed Rating: Consistently Implemented (Level 3)	

Function 2B: Protect - Identity and Access Management

Function	Count
Ad-Hoc	0
Defined	0
Consistently Implemented	4
Managed and Measurable	4
Optimized	0
<hr/>	
Calculated Rating: Managed and Measurable (Level 4)	
Assessed Rating: Managed and Measurable (Level 4)	

Function 2C: Protect - Data Protection and Privacy

Function	Count
Ad-Hoc	0
Defined	0
Consistently Implemented	2
Managed and Measurable	3
Optimized	0
<hr/>	
Calculated Rating: Managed and Measurable (Level 4)	

APPENDIX A: Maturity Model Scoring

Assessed Rating: Managed and Measurable (Level 4)

Function 2D: Protect - Security Training

Function	Count
Ad-Hoc	0
Defined	0
Consistently Implemented	2
Managed and Measurable	3
Optimized	0
<hr/>	
Calculated Rating: Managed and Measurable (Level 4)	
Assessed Rating: Managed and Measurable (Level 4)	

Function 3: Detect - ISCM

Function	Count
Ad-Hoc	0
Defined	0
Consistently Implemented	0
Managed and Measurable	4
Optimized	0
<hr/>	
Calculated Rating: Managed and Measurable (Level 4)	

Function 4: Respond - Incident Response

Function	Count
Ad-Hoc	0
Defined	0

APPENDIX A: Maturity Model Scoring

Consistently Implemented	4
Managed and Measurable	3
Optimized	0
<hr/>	
Calculated Rating: Consistently Implemented (Level 3)	

Function 5: Recover - Contingency Planning

Function	Count
Ad-Hoc	0
Defined	0
Consistently Implemented	4
Managed and Measurable	2
Optimized	0
<hr/>	
Calculated Rating: Consistently Implemented (Level 3)	

Overall

Function	Calculated Maturity Level	Accessed Maturity Level	Explanation
Function 1: Identify - Risk Management / Supply Chain Risk Management	Managed and Measurable (Level 4)	Ad Hoc (Level 1)	
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)	

APPENDIX A: Maturity Model Scoring

Function 5: Recover - Contingency Planning	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)
Overall	Effective	Effective

Appendix 4

Report Distribution

Federal Labor Relations Authority

Colleen Duffy Kiko, Member

James T. Abbott, Member

Michael Jeffries, Executive Director

Dave Fontaine, Chief Information Officer

Noah Peters, 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](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