Office of Inspector General

Evaluation of FLRA's Compliance with the FISMA FY 2023

EVALUATION OF THE FEDERAL LABOR RELATIONS AUTHORITY'S COMPLIANCE WITH THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT FISCAL YEAR 2023

Report No.
MAR-23-05 July 2023

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: Current Year Finding 3
Appendix 2: Management Response 6
Appendix 3: OIG Responses Reported in Cyberscope 7
Appendix 4: Report Distribution 8

Abbreviations

Dembo Jones	Dembo Jones, P.C.
FISMA	Federal Information Security Modernization Act
FLRA	Federal Labor Relations Authority
FY	Fiscal Year
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

DEMBO·JONES
CERTIFIED PUBLIC ACCOUNTANTS & ADVISORS

Evaluation of FLRA's Compliance with the FISMA FY 2023

Report No. MAR-23-05 ***July 27, 2023***

The Honorable Susan Tsui Grundmann
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) 2023 report to the Office of Management and Budget (OMB) and Congress.

Results in Brief

During our FY 2023 evaluation, we noted that the FLRA has taken significant steps to improve the information security program. We also noted that the FLRA does take information security weaknesses seriously. This year's testing identified *one* new finding, related to Policies. FLRA had no prior year issues to follow up on.

Background

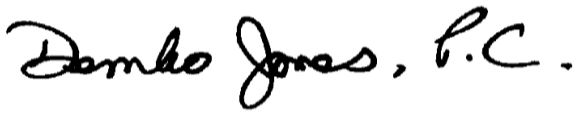
On December 17, 2002, the President signed into law H.R. 2458, the E-Government Act of 2002 (Public Law 107-347). Title III of the E-Government Act of 2002, commonly referred to as FISMA, focuses on improving oversight of Federal information security programs and facilitating progress in correcting agency 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 confidentially, 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.

North Bethesda, Maryland
July 27, 2023

Appendix 1
Current Year Finding

Although the FLRA has various information technology security policies and procedures, several had not been updated / reviewed in a timely manner, or they were lacking from development into a formalized policy. Specifically, the following was noted:

NIST Control	Deficiency
Personnel Security Policy and Procedures (PS-1)	There are no documented and approved Personnel Security Policies in accordance with NIST 800-53 Rev. 5.
Security Assessment and Authorization Policies and Procedures (CA-1)	Although the Security Assessment and Authorization Policy was developed, it wasn't approved in accordance with NIST 800-53 Rev. 5.
Identification and Authentication Policy and Procedures (IA-1)	There are no documented and approved Identification and Authentication Policies in accordance with NIST 800-53 Rev. 5.
Access Control Policy and Procedures (AC-1)	There are no documented and approved Access Control Policies in accordance with NIST 800-53 Rev. 5.

Criteria:
NIST 800-53, Revision 5, Personnel Security Policy (PS-1) states:
"The organization:

a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
    1. A personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
    2. Procedures to facilitate the implementation of the personnel security policy and associated personnel security controls; and
b. Reviews and updates the current:
    1. Personnel security policy [Assignment: organization-defined frequency]; and
    2. Personnel security procedures [Assignment: organization-defined frequency]."

NIST 800-53, Revision 5, Security Assessment and Authorization Policy (CA-1) states:
"The organization:

a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
    1. A security assessment and authorization policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

2. Procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls; and

b. Reviews and updates the current:
   1. Security assessment and authorization policy [Assignment: organization-defined frequency]; and
   2. Security assessment and authorization procedures [Assignment: organization-defined frequency]."

NIST 800-53, Revision 5, Identification and Authentication Policy and Procedures (IA-1) states:
"The organization:

a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. An identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls; and
b. Reviews and updates the current:
   1. Identification and authentication policy [Assignment: organization-defined frequency]; and
   2. Identification and authentication procedures [Assignment: organization-defined frequency]."

NIST 800-53, Revision 5, Access Control Policy and Procedures (AC-1) states:
"The organization:

a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the access control policy and associated access controls; and
b. Reviews and updates the current:
   1. Access control policy [Assignment: organization-defined frequency]; and
   2. Access control procedures [Assignment: organization-defined frequency]."

Cause:
Due to time constraints, FLRA did not adequately review and/or update as well ensure they have appropriate policies and procedures in accordance with NIST 800-53, Revision 5.

Effect:
Without finalized policies and procedures, there is an increased risk that IT staff will be unaware of the requirements when deploying and designing security controls.

Recommendation:

1. The FLRA CIO should develop, review and update, as necessary, the following information security program policies and procedures in accordance with NIST and agency requirements:

    a. Personnel Security policy.
    b. Security Assessment policy.
    c. Identification and Authentication policy.
    d. Access policy.

Management Response:

Management agrees with our recommendation.

UNITED STATES OF AMERICA
FEDERAL LABOR RELATIONS AUTHORITY

July 26, 2023

MEMORANDUM

TO: Dana Rooney, Inspector General

FROM: Dave Fontaine, Director Information Resources Management Division

THROUGH: Michael Jeffries, Executive Director

SUBJECT: Management Response to FY2023 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 "***Evaluation of FLRA's Compliance with the FISMA FY 2023.***" The Federal Labor Relations Authority (FLRA) appreciates the very in-depth review of our information security program, and that, despite a host of new controls being evaluated, that there was only *one* recommendation issued.

RECOMMENDATION FOR FINDING RE: POLICIES

1. *The FLRA should develop, review and update, as necessary, the following information security program policies and procedures in accordance with NIST and agency requirements:*

    a. *Personnel Security policy.*
    b. *Security Assessment policy.*
    c. *Identification and Authentication policy.*
    d. *Access policy.*

Management Response: As the report mentions, the very recent revisions to the NIST 800-53 (*Rev 5*) were not reflected in the current versions of our policies. We are a small Agency with extremely limited resources, but we take Information Security very seriously. 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 listed policy documents are updated, thoroughly reviewed, and enacted timely.

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

Appendix 3
OIG Responses Reported in Cyberscope

Inspector General

Section Report

2023

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.

Please refer to the final report.

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?

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?

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?

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, including for high value assets?

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?

Managed and Measurable (Level 4)

6 To what extent does the organization use an information security architecture to provide a disciplined and structured methodology for managing risk, including risk from the organization's supply chain?

7 To what extent have the roles and responsibilities of internal and external stakeholders involved in cybersecurity risk management processes been defined, communicated, implemented, and appropriately resourced across the organization?

Managed and Measurable (Level 4)

8 To what extent has the organization ensured that plans of action and milestones (POA&Ms) are used for effectively mitigating security weaknesses?

Consistently Implemented (Level 3)

Comments : There was no integration into ERM.

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?

Consistently Implemented (Level 3)

Comments : No measurement of qualitative and quantitative measures on SRCM.

10 To what extent does the organization use 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?

Consistently Implemented (Level 3)

Comments : No integration into ERM.

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 organizations 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?

Nothing to add.

Function 1B: Identify - Supply Chain Risk Management

12 To what extent does the organization use 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?

Consistently Implemented (Level 3)

Comments : No automated mechanisms.

13 To what extent does the organization use SCRM policies and procedures to manage SCRM activities at all organizational tiers?

Consistently Implemented (Level 3)

Comments : No automated mechanisms.

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?

Consistently Implemented (Level 3)

Comments : There are no qualitative and quantitative measurements.

15 To what extent does the organization ensure that counterfeit components are detected and prevented from entering the organization’s systems?

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

Consistently Implemented (Level 3)

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

Consistently Implemented (Level 3)

16.3 Provide any additional information on the effectiveness (positive or negative) of the organizations 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?

Nothing to add.

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?

18 To what extent does the organization use 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 contractoroperated systems?

19

To what extent does the organization use baseline configurations for its information systems and maintain inventories of related components at a level of granularity necessary for tracking and reporting?

Consistently Implemented (Level 3)

Comments : No automated mechanisms.

20 To what extent does the organization use configuration settings/common secure configurations for its information systems?

Consistently Implemented (Level 3)

Comments : No automated mechanisms.

21 To what extent does the organization use flaw remediation processes, including asset discovery, vulnerability scanning, analysis, and patch management, to manage software vulnerabilities on all network addressable IP- assets?

Consistently Implemented (Level 3)

Comments : Flaw remediation is not centrally managed.

22 To what extent has the organization adopted the Trusted Internet Connection (TIC) program to assist in protecting its network?

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, asappropriate?

24 To what extent does the organization use a vulnerability disclosure policy (VDP) as part of its vulnerability management program for internet- accessible federal systems?

Consistently Implemented (Level 3)

Comments : There are no qualitative and quantitative measures.

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 organizations 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?

Nothing to add.

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?

Ad Hoc (Level 1)

Comments : Roles are not defined and implemented throughout the agency.

27 To what extent does the organization use a comprehensive ICAM policy, strategy, process, and technology solution roadmap to guide its ICAM processes and activities?

Ad Hoc (Level 1)

Comments : A comprehensive ICAM Policy is not deployed throughout the agency.

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?

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?

Managed and Measurable (Level 4)

30 To what extent has the organization implemented phishing-resistant multifactor authentication mechanisms (e.g., PIV, FIDOor web authentication) for non- privileged users to access the organization`s facilities [organization-defined entry/exit points], networks, and systems, including for remote access?

Managed and Measurable (Level 4)

31 To what extent has the organization implemented phishing-resistant multifactor authentication mechanisms (e.g., PIV, FIDOor web authentication) for privileged users to access the organization`s facilities [organization-defined entry/exit points], networks, and systems, including for remote access?

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?

Consistently Implemented (Level 3)

Comments : No automated mechanisms.

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 accesssessions?

Managed and Measurable (Level 4)

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

Consistently Implemented (Level 3)

34.2 Provide any additional information on the effectiveness (positive or negative) of the organizations 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?

Nothing to add.

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?

Consistently Implemented (Level 3)

Comments : There are no qualitative and quantitative performance measures.

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?
 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 (e.g., EDR) to prevent data exfiltration and enhance network defenses?

Consistently Implemented (Level 3)

Comments : No quantitative and qualitative measures.

38 To what extent has the organization developed and implemented a Data Breach Response Plan, as appropriate, to respond to privacy events?

39 To what extent does the organization ensure that privacy awareness training is provided to all individuals, including role-based privacy training?(Note: Privacy awareness training topics should include, as appropriate: responsibilities under the Privacy Act of and E- Government Act of 20consequences for failing to carry out responsibilities, identifying privacy risks, mitigating privacy risks, and reporting privacy incidents, data collections and userequirements)

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

Consistently Implemented (Level 3)

40.2 Provide any additional information on the effectiveness (positive or negative) of the organizations 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?

Nothing to add.

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 securityresponsibilities.

Managed and Measurable (Level 4)

42 To what extent does the organization use 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?

Managed and Measurable (Level 4)

43

To what extent does the organization use 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
 Deployment methods

Managed and Measurable (Level 4)

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?

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)?

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 organizations 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?

Nothing to add.

Function 3: Detect - ISCM

47 To what extent does the organization use information security continuous monitoring (ISCM) policies and an ISCM strategy that addresses ISCM requirements and activities at each organizational tier?

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?

Ad Hoc (Level 1)

Comments : The ISCM structure hasn't been defined.

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?

Managed and Measurable (Level 4)

50 How mature is the organization`s process for collecting and analyzing ISCM performance measures and reporting findings?

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

Consistently Implemented (Level 3)

51.2 Provide any additional information on the effectiveness (positive or negative) of the organizations 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?

Nothing to add.

Function 4: Respond - Incident Response

52

To what extent does the organization use an incident response plan to provide a formal, focused, and coordinated approach to responding to incidents?

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?

54 How mature are the organization`s processes for incident detection and analysis?

Consistently Implemented (Level 3)

Comments : No qualitative and quantitative measurements.

55 How mature are the organization`s processes for incident handling?

Consistently Implemented (Level 3)

Comments : No qualitative and quantitative performance measures.

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?

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?

Consistently Implemented (Level 3)

Comments : Einstein 3 is not being deployed.

58

To what extent does the organization use 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 serversecurity tools

Managed and Measurable (Level 4)

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

Consistently Implemented (Level 3)

59.2 Provide any additional information on the effectiveness (positive or negative) of the organizations 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?

Nothing to add.

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?

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?

Managed and Measurable (Level 4)

62 To what extent does the organization ensure that information system contingency plans are developed, maintained, and integrated with other continuity plans?

63 To what extent does the organization perform tests/exercises of its information system contingency planning processes?

Managed and Measurable (Level 4)

64 To what extent does the organization perform information system backup and storage, including use of alternate storage and processing sites, as appropriate?

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 teamsand used to make risk- based decisions?

Managed and Measurable (Level 4)

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

Managed and Measurable (Level 4)

66.2 Provide any additional information on the effectiveness (positive or negative) of the organizations 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?

Nothing to add.

APPENDIX A: Maturity Model Scoring

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

Function	Core	FY23 Supplemental	FY24 Supplemental	FY23 Assessed Maturity	FY23 Effectivness	Explanation
Identify	3.83	3.20	N/A	Consistently Implemented (Level 3)		
Protect	3.50	3.10	N/A	Managed and Measurable (Level 4)		
Detect	4.00	1.00	N/A	Consistently Implemented (Level 3)		
Respond	3.00	3.50	N/A	Consistently Implemented (Level 3)		
Recover	4.00	4.00	N/A	Managed and Measurable (Level 4)		
Overall Maturity	**3.67**	**2.96**	**N/A**			

Function 1A: Identify - Risk Management

Maturity Level	Core	Supplemental
Ad Hoc (Level 1)	0	0
Defined (Level 2)	0	0
Consistently Implemented (Level 3)	1	2

Managed and Measurable (Level 4)	3	1
Optimized (Level 5)	1	0
Calculated Rating:	**4.00**	**3.33**

Function 1B: Identify - Supply Chain Risk Management

Maturity Level	Core	Supplemental
Ad Hoc (Level 1)	0	0
Defined (Level 2)	0	0
Consistently Implemented (Level 3)	1	2
Managed and Measurable (Level 4)	0	0
Optimized (Level 5)	0	0
Calculated Rating:	**3.00**	**3.00**

Function 2A: Protect - Configuration Management

Maturity Level	Core	Supplemental
Ad Hoc (Level 1)	0	0
Defined (Level 2)	0	0
Consistently Implemented (Level 3)	2	2
Managed and Measurable (Level 4)	0	1

Optimized (Level 5)	0	0
Calculated Rating:	**3.00**	**3.33**

Function 2B: Protect - Identity and Access Management

Maturity Level	Core	Supplemental
Ad Hoc (Level 1)	0	2
Defined (Level 2)	0	0
Consistently Implemented (Level 3)	1	0
Managed and Measurable (Level 4)	2	2
Optimized (Level 5)	0	0
Calculated Rating:	**3.67**	**2.50**

Function 2C: Protect - Data Protection and Privacy

Maturity Level	Core	Supplemental
Ad Hoc (Level 1)	0	0
Defined (Level 2)	0	0
Consistently Implemented (Level 3)	1	1
Managed and Measurable (Level 4)	1	0
Optimized (Level 5)	0	0

Calculated Rating:	**3.50**	**3.00**

Function 2D: Protect - Security Training

Maturity Level	Core	Supplemental
Ad Hoc (Level 1)	0	0
Defined (Level 2)	0	0
Consistently Implemented (Level 3)	0	0
Managed and Measurable (Level 4)	1	2
Optimized (Level 5)	0	0
Calculated Rating:	**4.00**	**4.00**

Function 3: Detect - ISCM

Maturity Level	Core	Supplemental
Ad Hoc (Level 1)	0	1
Defined (Level 2)	0	0
Consistently Implemented (Level 3)	0	0
Managed and Measurable (Level 4)	2	0
Optimized (Level 5)	0	0
Calculated Rating:	**4.00**	**1.00**

Function 4: Respond - Incident Response

Maturity Level	Core	Supplemental
Ad Hoc (Level 1)	0	0
Defined (Level 2)	0	0
Consistently Implemented (Level 3)	2	1
Managed and Measurable (Level 4)	0	1
Optimized (Level 5)	0	0
Calculated Rating:	**3.00**	**3.50**

Function 5: Recover - Contingency Planning

Maturity Level	Core	Supplemental
Ad Hoc (Level 1)	0	0
Defined (Level 2)	0	0
Consistently Implemented (Level 3)	0	0
Managed and Measurable (Level 4)	2	2
Optimized (Level 5)	0	0
Calculated Rating:	**4.00**	**4.00**

Appendix 4
Report Distribution

Federal Labor Relations Authority

Colleen Duffy Kiko, Member
Michael Jeffries, Executive Director
Dave Fontaine, Chief Information Officer
Thomas Tso, Solicitor

CONTACTING THE OFFICE OF INSPECTOR GENERAL

IF YOU BELIEVE AN ACTIVITY IS WASTEFUL, FRAUDULENT, OR ABUSIVE OF FEDERAL FUNDS, CONTACT THE:

HOTLINE (877) 740-8278

HTTP://WWW.FLRA.GOV/OIG-HOTLINE

EMAIL: OIGMAIL@FLRA.GOV
CALL: (771) 444-5712 FAX: (202) 208-4535
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