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 2020

Report No. MAR-21-01

October 2020

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

CONTENTS

Evaluation Report

Appendices

Abbreviations

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

DEMBO·JONES
CERTIFIED PUBLIC ACCOUNTANTS & ADVISORS

Evaluation of FLRA's Compliance with the FISMA FY 2020

Report No. MAR-21-01 ***October 30, 2020***

The Honorable Colleen Duffy Kiko
Chairman

Dembo Jones, P.C. (Dembo Jones), on behalf of the Federal Labor Relations Authority (FLRA), Office of Inspector General (OIG), conducted an independent evaluation of the quality and compliance of the FLRA security program with applicable Federal computer security laws and regulations. Dembo Jones' evaluation focused on FLRA's information security required by the Federal Information Security Modernization Act (FISMA). The weaknesses discussed in this report should be included in FLRA's Fiscal Year (FY) 2020 report to the Office of Management and Budget (OMB) and Congress.

Results in Brief

During our FY 2020 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. This year's testing identified four weaknesses and we have made five recommendations. There were no prior year weaknesses.

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 (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.

Dembo Jones, P.C.

North Bethesda, Maryland
October 30, 2020

Appendix 1
Current Year Recommendations

01 Policies and Procedures

Condition:
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
Risk Assessment Policy and Procedures (RA-1)	Risk policy and procedures have not been formalized, reviewed and approved.
System and Services Acquisition Policy and Procedures (SA-1) & Acquisition Process (SA-4)	Update the Acquisition policy to ensure that it contains stipulations that require external service providers meet or exceed the NIST security requirements.
Personnel Security Policy and Procedures (PS-1)	FLRA's Personnel Security policy and procedures have not been formalized, reviewed and approved..
Security Assessment and Authorization Policy and Procedures (CA-1)	FLRA's Security Assessment policy and procedures formalized, reviewed and approved.
Configuration Management Policy and Procedures (CM-1 & CM-9)	The Configuration Management Plan and policy has not been formalized, reviewed and approved.
Incident Response Policy and Procedures (IR-1)	The Incident Response policy has not been formalized, reviewed and approved.
Security Awareness and Training Policy and Procedures (AT-1)	The Security Awareness policy has not been The Configuration Management policy has not been formalized, reviewed and approved.
Identification and Authentication Policy and Procedures (IA-1)	The Identification and Authentication policy has not been formalized, reviewed and approved.
Access Control Policy and Procedures (AC-1)	The Access Control Policy has not been formalized, reviewed and approved.
Mobile Code (SC-18)	Mobile code technologies and usage restrictions have not been formally documented in a Policy.

Criteria:
NIST 800-53, Revision 4, Risk Assessment Policy and Procedures (RA-1) states:
"The organization:

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

    2. Procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls; and
b. Reviews and updates the current:
    1. Risk assessment policy [*Assignment: organization-defined frequency*]; and
    2. Risk assessment procedures [*Assignment: organization-defined frequency*]."

<u>NIST 800-53, Revision 4, System and Services Acquisition Policy and Procedures (SA-1) states:</u>
"The organization:

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

<u>NIST 800-53, Revision 4, Acquisition Process (SA-4) states:</u>
"The organization:

a. Includes the following requirements, descriptions, and criteria, either explicitly or by reference, in information system acquisition contracts based on applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs:
    1. Security functional requirements;
    2. Security strength requirements;
    3. Security assurance requirements;
    4. Security-related documentation requirements;
    5. Description of the information system development environment and environment in which the system is intended to operate; and
    6. Acceptance criteria."

<u>NIST 800-53, Revision 4, Personnel Security Policy (PS-1) states:</u>
"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]."

<u>NIST 800-53, Revision 4, Security Assessment and Authorization Policy (CA-1) states:</u>
"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]."

<u>NIST 800-53, Revision 4, Configuration Management Policy and Procedures (CM-1) states:</u>
"The organization:

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

<u>NIST 800-53, Revision 4, Configuration Management Plan (CM-9) states:</u>
"The organization develops, documents, and implements a configuration management plan for the information system that:

a. Addresses roles, responsibilities, and configuration management processes and procedures;

b. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items;
c. Defines the configuration items for the information system and places the configuration items under configuration management; and
d. Protects the configuration management plan from unauthorized disclosure and modification."

NIST 800-53, Revision 4, Incident Response Policy and Procedures (IR-1) states:
"The organization:

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

NIST 800-53, Revision 4, Security Awareness and Training Policy and Procedures (AT-1) states:
"The organization:

a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
    1. A security awareness and training 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 awareness and training policy and associated security awareness and training controls; and
b. Reviews and updates the current:
    1. Security awareness and training policy [Assignment: organization-defined frequency]; and
    2. Security awareness and training procedures [Assignment: organization-defined frequency]."

NIST 800-53, Revision 4, 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]."

<u>NIST 800-53, Revision 4, Access Control Policy and Procedures (AC-1) states:</u>
"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]."

<u>NIST 800-53, Revision 4, Mobile Code (SC-18) states:</u>
"The organization:

a. Defines acceptable and unacceptable mobile code and mobile code technologies;
b. Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and
c. Authorizes, monitors, and controls the use of mobile code within the information system."

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 4.

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.

Recommendations:

1. 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. Personnel Security policy.
f. Configuration Management policy.
g. Configuration Management Plan.
h. Incident Response policy.
i. Security Awareness policy.
j. Identification and Authentication policy.
k. Access policy.
l. Mobile Code Usage and Restrictions Policy

Management Response:

Management agrees with our recommendation.

02 Timely Remediation of Vulnerabilities

Condition:
We reviewed three vulnerability scan results over an eight month period to assess the timely remediation of vulnerabilities. The following was the result of that review:

1st Scan
High vulnerability – 2
Medium vulnerabilities – 9

2nd Scan
High vulnerability – 2
Medium vulnerabilities – 10

3rd Scan
High vulnerability – 2
Medium vulnerabilities – 11

Based on the above evaluation results, the same high and medium vulnerabilities from the first scan had not been remediated in the subsequent scan. Therefore, the high and medium vulnerabilities are not being remediated in a timely manner in order to protect the agency from known or unforeseen exposures and exploitation.

Criteria:
NIST 800-53, Revision 4, Risk Assessment (RA)-5 states:
According to NIST, the organization "remediates legitimate vulnerabilities in accordance with an organizational assessment of risk."

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

Risk:
By having high and medium vulnerabilities exposed to the agency, and not remediated in a timely manner, there is the risk that adversaries can take advantage of those weaknesses and gain access to FLRA's data, which ultimately may lead to a lack of integrity and/or confidentiality for the agency.

Recommendation(s):

2. 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.

Management Response:

Management agrees with our recommendation.

03 Position Description

Condition:
FLRA does not maintain a listing of all positions reconciling against their risk designation.

Criteria:
NIST 800-53, Revision 4, Position Risk Designation (PS-2) states:
“The organization:

1. Assigns a risk designation to all organizational positions;
2. Establishes screening criteria for individuals filling those positions; and
3. Reviews and updates position risk designations [Assignment: organization-defined frequency].”

Cause:
Due to a lack of personnel, budget, or time constraints, FLRA did not adequately map each position to a risk designation for maintaining the overall security posture.

Effect:
Without assigning risks to each position, the IT management and staff will be unable to appropriately secure the systems because auditing and logging will not be focused in areas of concern or increased risk.

Recommendation:

3. 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.

Management Response:

Management agrees with our recommendation.

04 Account Management

Condition:
Upon review of a sampled set of users for their access authorizations, the following was noted:

- There was no evidence to conclude that an annual recertification of users' access rights was being performed.
- Admin users were not being reviewed on a semi-annual basis.

Criteria:

NIST 800-53, Revision 4, Access Control (AC)-2 states:
"Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account."

"Authorizes access to the information system based on:
1. A valid access authorization;
2. Intended system usage; and
3. Other attributes as required by the organization or associated missions/business functions."

Cause:

Due to a lack of personnel, budget, or time constraints, FLRA did not adequately document and/or ensure that everyone's access was appropriately approved.

Effect:

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

Recommendations:

4. 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. On a semi-annual basis, all admin users' account should be reviewed to ensure their authorizations are still appropriate.

Management Response:

Management agrees with our recommendation.

Appendix 2
Management Response

UNITED STATES OF AMERICA
FEDERAL LABOR RELATIONS AUTHORITY

October 29, 2020

MEMORANDUM

TO: Dana Rooney
Inspector General

FROM: Michael Jeffries
Executive Director

SUBJECT: Management Response to FY2020 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 2020.***”. 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, only 4 findings have been reported. A 99.6% success rate for any agency would be a crowning achievement, but for a small/micro agency, it is truly a proud reflection of FLRA’s commitment to the program.

We concur with the 5 recommendations associated with the 4 findings in the draft report, and we look forward to shoring up the shortcomings with speed and efficiency.

Recommendations for Finding No. 01 – Policies and Procedures

1. *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. *Personnel Security policy.*
    f. *Configuration Management policy.*
    g. *Configuration Management Plan.*
    h. *Incident Response policy.*
    i. *Security Awareness policy.*
    j. *Identification and Authentication policy.*
    k. *Access policy.*
    l. *Mobile Code Usage and Restrictions Policy*

Management Response: The Executive Director concurs with the recommendations and will work with the Director of the Information Resources Management Division (IRMD) to *develop, review and update* policies and procedures as necessary. Of note, the majority of the processes and policies referenced are already in practice, but the finding reflects that these practices need to be properly documented. The Agency has already begun to draft the identified documents.

<u>Recommendations for Finding No. 02 – Timely Remediation of Vulnerabilities</u>

2. *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.*

Management Response: The Executive Director concurs with the recommendations. The Agency has already begun to draft a formalized policy regarding the timely remediation of deficiencies, which will include a better description of why – as in the case of some of the deficiencies identified – deficiencies might *not* be remediated within the "best practices" guidelines noted in the recommendations (e.g. if immediate remediation would put unrealistic financial burden on the Agency).

<u>Recommendations for Finding No. 03 – Position Description</u>

3. *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.*

Management Response: The Executive Director concurs with the recommendations and will work with the Directors of IRMD and the Human Resources Division (HRD) to perform a comprehensive analysis and risk classification. That information and documentation will then be used to inform the decision-making process for areas of concern.

<u>Recommendations for Finding No. 04 – Account Management</u>

4. *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. *On a semi-annual basis, all admin users' account should be reviewed to ensure their authorizations are still appropriate.*

Management Response: The Executive Director concurs with the recommendations. The FLRA generally reviews account access in compliance with these recommendations, but will ensure these semi-annual and annual review requirements are incorporated into the agency policy and effectively documented.

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.

For Official Use Only

Inspector General

Section Report

2020

Annual FISMA
Report

Federal Labor Relations Authority

For Official Use Only

Function 1: Identify - Risk Management

1 To what extent does the organization maintain a comprehensive and accurate inventory of its information systems (including cloud systems, public facing websites, and third party systems), and system interconnections (NIST SP 800-53. Rev. 4: CA-3, PM-5, and CM-8; NIST 800-161; NIST Cybersecurity Framework (CSF): ID.AM-1 - 4; FY 2020 CIO FISMA Metrics: 1.1 and 1.4, OMB A-130).

Managed and Measurable (Level 4)

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; NISTIR 8011; Federal Enterprise Architecture (FEA) Framework, v2; FY 2020 CIO FISMA Metrics: 1.2

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; NISTIR 8011; FEA Framework, v2; FY 2020 CIO FISMA Metrics: 1.2.5, 1.3.3, 3.10; CSF: ID.AM-2)?

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 (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 2020 CIO FISMA Metrics: 1.1; OMB M-19-03)?

Managed and Measurable (Level 4)

5 To what extent has the organization established, communicated, and implemented its risk management policies, procedures, and strategy, including for supply chain risk management. This includes the organization's processes and methodologies for categorizing risk, developing a risk profile, assessing risk, risk appetite/tolerance levels, responding to risk, and monitoring risk (NIST SP 800-39; NIST SP 800-53 Rev. 4: PM-8, PM-9; CSF: ID RM-1 - ID.RM-3; OMB A-123; OMB M-16-17; Green Book (Principle #6); CFO Council ERM Playbook; OMB M-17-25; NIST SP 800-37 (Rev. 2); NIST SP 800-161: Appendix E; CSF: ID.SC-1 - 2; SECURE Technology Act: s. 1326, Executive Order 13873, Securing the Information and Communications Technology and Services Supply Chain, May 15, 2019)?

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); 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 800-161; NIST SP 800-163, Rev. 1 CSF: ID.SC-1 and PR.IP-2; SECURE Technology Act: s. 1326)?

Managed and Measurable (Level 4)

Function 1: Identify - Risk Management

7 To what degree have roles and responsibilities of internal and external stakeholders involved in risk management processes been defined and communicated across the organization (NIST SP 800-39: Section 2.3.1 and 2.3.2; NIST SP 800-53 Rev. 4: RA-1; CSF: ID.AM-6, ID.RM-1, and ID.GV-2; OMB A-123; CFO Council ERM Playbook; NIST SP 800-37 (Rev. 2); 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); OMB M-19-03, CSF v1.1, ID.RA-6)?

Managed and Measurable (Level 4)

9 To what extent has the organization defined, communicated, and implemented its policies and procedures for conducting system level risk assessments, including for identifying and prioritizing (i) internal and external threats, including through use of the common vulnerability scoring system, or other equivalent framework (ii) internal and external asset vulnerabilities, including through vulnerability scanning, (iii) the potential likelihoods and business impacts/consequences of threats exploiting vulnerabilities, and (iv) security controls to mitigate system-level risks (NIST SP 800-39; NIST SP 800-53 REV. 4: PL-2 and RA-1; NIST SP 800-30; CSF: Section 4.0; NIST SP 800-37 (Rev. 2))?

Managed and Measurable (Level 4)

10 To what extent does the organization ensure that information about risks are communicated in a timely manner to all necessary internal and external stakeholders (CFO Council ERM Playbook; OMB A-123; OMB Circular A-11; Green Book (Principles #9, #14 and #15); OMB M-19-03; CSF: Section 3.3; SECURE Technology Act: s. 1326)?

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 (NIST SP 800-53 REV. 4: SA-4; NIST SP 800-152; NIST SP 800-37 Rev. 2; FedRAMP standard contract clauses; Cloud Computing Contract Best Practices; OMB M-19-03; OMB A-130; CSF: ID.SC-2 through 4).

Ad Hoc (Level 1)

Comments: The organization has not defined a process that includes information security and other business areas as appropriate for ensuring that contracts and other agreements for third party systems and services include appropriate clauses to monitor the risks related to such systems and services. In addition, the organization has defined its processes to ensure that security controls of systems or services provided by contractors or other entities on behalf of the organization meet FISMA requirements, OMB policy, and applicable NIST guidance.

Function 1: Identify - Risk Management

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

Ad Hoc (Level 1)

Comments: The organization doesn't consistently implement an automated solution across the enterprise that provides a centralized, enterprise wide view of risks, including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards.

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

Managed and Measurable (Level 4)

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?

Refer to report draft.

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 REV. 4: CM-1; NIST SP 800-128: Section 2.4)?

Ad Hoc (Level 1)

Comments: Roles and responsibilities at the organizational and information system levels for stakeholders involved in information system configuration management have not been fully defined and communicated across the organization.

15 To what extent does the organization utilize an enterprise wide configuration management plan that includes, at a minimum, the following components: roles and responsibilities, including establishment of a Change Control Board (CCB) or related body; configuration management processes, including processes for: identifying and managing configuration items during the appropriate phase within an organization's SDLC; configuration monitoring; and applying configuration management requirements to contractor operated systems (NIST SP 800-128: Section 2.3.2; NIST SP 800-53 REV. 4: CM-9)?

Ad Hoc (Level 1)

Comments: The organization has not developed an organization wide configuration management plan that includes the necessary components.

Function 2A: Protect - Configuration Management

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 REV. 4: CM-1; NIST SP 800-128: 2.2.1)

Ad Hoc (Level 1)

Comments: The organization has not developed, documented, and disseminated comprehensive policies and procedures for managing the configurations of its information systems.

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 REV. 4: CM-2 and CM-8; FY 2020 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: The organization doesn't employ automated mechanisms (such as application whitelisting and network management tools) to detect unauthorized hardware, software, and firmware on its network and take immediate actions to limit any security impact.

18 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 2020 CIO FISMA Metrics: 2.1, 2.2, 2.14, 4.3; SANS/CIS Top 20 Security Controls 3.7; CSF: ID.RA-1 and DE.CM-8)?

Ad Hoc (Level 1)

Comments: The organization has not developed, documented, and disseminated its policies and procedures for configuration settings/common secure configurations. In addition, the organization has developed, documented, and disseminated common secure configurations (hardening guides) that are tailored to its environment.

19 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 2020 CIO FISMA Metrics: 1.3.7, 1.3.8, 2.13, 2.14; CSF: ID.RA-1; DHS Binding Operational Directive (BOD) 15-01; DHS BOD 18-02)?

Consistently Implemented (Level 3)

Comments: The organization doesn't centrally manages its flaw remediation process and utilizes automated patch management and software update tools for operating systems, where such tools are available and safe.

20 To what extent has the organization adopted the Trusted Internet Connection (TIC) program to assist in protecting its network (OMB M-19-26)

Managed and Measurable (Level 4)

Function 2A: Protect - Configuration Management

21 To what extent has the organization defined and implemented configuration change control activities including: determination of the types of changes that are configuration controlled; review and approval/disapproval of proposed changes with explicit consideration of security impacts and security classification of the system; documentation of configuration change decisions; implementation of approved configuration changes; retaining records of implemented changes; auditing and review of configuration changes; and coordination and oversight of changes by the CCB, as appropriate (NIST SP 800-53 REV. 4: CM-2, CM-3 and CM-4; CSF: PR.IP-3).

Consistently Implemented (Level 3)

Comments: The organization doesn't monitor, analyze, and report qualitative and quantitative performance measures on the effectiveness of its change control activities and ensures that data supporting the metrics is obtained accurately, consistently, and in a reproducible format.

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?

Refer to report draft.

Calculated Maturity Level - Ad Hoc (Level 1)

Function 2B: Protect - Identity and Access Management

23 To what degree have the roles and responsibilities of identity, credential, and access management (ICAM) stakeholders been defined, communicated across the agency, and appropriately resourced (NIST SP 800-53 REV. 4: AC-1, IA-1, and PS-1; Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance (FICAM))?

Ad Hoc (Level 1)

Comments: Roles and responsibilities at the organizational and information system levels for stakeholders involved in ICAM have not been fully defined and communicated across the organization.

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

Ad Hoc (Level 1)

Comments: The organization has not defined its ICAM strategy and developed milestones for how it plans to align with Federal initiatives, including strong authentication, the FICAM, OMB M-19-17, segment architecture, and phase 2 of DHS's Continuous Diagnostics and Mitigation (CDM) program, as appropriate.

Function 2B: Protect - Identity and Access Management

25 To what degree have ICAM policies and procedures been defined and implemented? (Note: the maturity level should take into consideration the maturity of questions 26 through 31) (NIST SP 800-53 REV. 4: AC-1 and IA-1; Cybersecurity Strategy and Implementation Plan (CSIP); SANS/CIS Top 20: 14.1; DHS ED 19-01; CSF: PR.AC-4 and 5)?

Ad Hoc (Level 1)

Comments: The organization has not developed, documented, and disseminated its policies and procedures for ICAM.

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 REV. 4: PS-2 and PS-3; National Insider Threat Policy; CSF: PR.IP-11)?

Ad Hoc (Level 1)

Comments: The organization has not defined its processes for ensuring that all personnel are assigned risk designations and appropriately screened prior to being granted access to its systems.

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 REV. 4: AC-8, PL-4, and PS6)?

Managed and Measurable (Level 4)

28 To what extent has the organization implemented strong authentication mechanisms (PIV or a 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 REV. 4: AC-17; NIST SP 800-128; FIPS 201-2; NIST SP 800-63; FY 2019 CIO FISMA Metrics: 2.4 and 2.7; CSF: PR.AC-1 and 6; and Cybersecurity Sprint)?

Optimized (Level 5)

29 To what extent has the organization implemented strong authentication mechanisms (PIV or a 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 REV. 4: AC-17; NIST SP 800-128; FIPS 201-2; NIST SP 800-63; FY 2019 CIO FISMA Metrics: 2.3, 2.5, and 2.7; CSF: PR.AC-1 and 6; DHS ED 19-01; and Cybersecurity Sprint)?

Optimized (Level 5)

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 2019 CIO FISMA Metrics: 2.3 and 2.5; NIST SP 800-53 REV. 4: AC-1, AC-2 (2), and AC-17; CSIP; DHS ED 19- 01; CSF: PR.AC-4).

Ad Hoc (Level 1)

Comments: The organization has not defined its processes for provisioning, managing, and reviewing privileged accounts.

Function 2B: Protect - Identity and Access Management

31 To what extent does the organization ensure that appropriate configuration/connection requirements are maintained for remote access connections? This includes the use of appropriate cryptographic modules, system time-outs, and the monitoring and control of remote access sessions (NIST SP 800-53 REV. 4: AC-17 and SI-4; CSF: PR.AC-3; and FY 2019 CIO FISMA Metrics: 2.10)?.

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?

Refer to report draft.

Calculated Maturity Level - Ad Hoc (Level 1)

Function 2C: Protect - Data Protection and Privacy

33 To what extent has the organization developed a privacy program for the protection of personally identifiable information (PII) that is collected, used, maintained, shared, and disposed of by information systems (NIST SP 800-122; NIST SP 800-37 (Rev. 2); OMB M-18- 02; OMB M-19-03; OMB A-130, Appendix I; CSF: ID.GV-3; NIST SP 800-53 REV. 4: AR-4 and Appendix J)?

Managed and Measurable (Level 4)

34 To what extent has the organization implemented the following security controls to protect its PII and other agency sensitive data, as appropriate, throughout the data lifecycle? (NIST SP 800-53 REV. 4; Appendix J, SC-8, SC-28, MP-3, and MP-6; NIST SP 800-37 (Rev. 2); FY 2019 CIO FISMA Metrics: 2.8; 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

Consistently Implemented (Level 3)

Comments: The organization doesn't ensure that the security controls for protecting PII and other agency sensitive data, as appropriate, throughout the data lifecycle are subject to the monitoring processes defined within the organization's ISCM strategy.

35 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 2019 CIO FISMA Metrics: 3.8; DHS BOD 18-01; DHS ED 19-01; CSF: PR.DS-5)?

Consistently Implemented (Level 3)

Comments: The organization doesn't analyze qualitative and quantitative measures on the performance of its data exfiltration and enhanced network defenses.

Function 2C: Protect - Data Protection and Privacy

36 To what extent has the organization developed and implemented a Data Breach Response Plan, as appropriate, to respond to privacy events? (NIST SP 800-122; NIST SP 800-53 REV. 4: Appendix J, SE-2; FY 2018 SAOP FISMA metrics; OMB M-17-12; and OMB M-17- 25)?

Managed and Measurable (Level 4)

37 To what degree does the organization ensure that privacy awareness training is provided to all individuals, including role-based privacy training (NIST SP 800-53 REV. 4: AR-5)? (Note: Privacy awareness training topics should include, as appropriate: responsibilities under the Privacy Act of 1974 and E-Government Act of 2002, consequences for failing to carry out responsibilities, identifying privacy risks, mitigating privacy risks, and reporting privacy incidents, data collections and use requirements)

Optimized (Level 5)

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

Refer to report draft.

Calculated Maturity Level - Managed and Measurable (Level 4)

Function 2D: Protect - Security Training

39 To what degree have the roles and responsibilities of security awareness and training program stakeholders been defined, communicated across the agency, and appropriately resourced? (Note: this includes the roles and responsibilities for the effective establishment and maintenance of an organization wide security awareness and training program as well as the awareness and training related roles and responsibilities of system users and those with significant security responsibilities (NIST SP 800- 53 REV. 4: AT-1; and NIST SP 800-50).

Defined (Level 2)

Comments: Individuals are not performing the roles and responsibilities that have been defined across the organization.

40 To what extent does the organization utilize an assessment of the skills, knowledge, and abilities of its workforce to provide tailored awareness and specialized security training within the functional areas of: identify, protect, detect, respond, and recover (NIST SP 800-53 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)

Function 2D: Protect - Security Training

41 To what extent does the organization utilize a security awareness and training strategy/plan that leverages its organizational skills assessment and is adapted to its culture? (Note: the strategy/plan should include the following components: the structure of the awareness and training program, priorities, funding, the goals of the program, target audiences, types of courses/material for each audience, use of technologies (such as email advisories, intranet updates/wiki pages/social media, web based training, phishing simulation tools), frequency of training, and deployment methods (NIST SP 800-53 REV. 4: AT-1; NIST SP 800-50: Section 3; CSF: PR.AT- 1).

Managed and Measurable (Level 4)

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

Managed and Measurable (Level 4)

43 To what degree does the organization ensure that security awareness training is provided to all system users and is tailored based on its organizational requirements, culture, and types of information systems? (Note: awareness training topics should include, as appropriate: consideration of organizational policies, roles and responsibilities, secure e-mail, browsing, and remote access practices, mobile device security, secure use of social media, phishing, malware, physical security, and security incident reporting (NIST SP 800-53 REV. 4: AT-2; FY 2019 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)

44 To what degree does the organization ensure that specialized security training is provided to all individuals with significant security responsibilities (as defined in the organization's security policies and procedures) (NIST SP 800- 53 REV. 4: AT-3 and AT-4; FY 2019 CIO FISMA Metrics: 2.15)?

Managed and Measurable (Level 4)

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

Managed and Measurable (Level 4)

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

Refer to report draft.

Calculated Maturity Level - Managed and Measurable (Level 4)

Function 3: Detect - ISCM

Function 3: Detect - ISCM

46 To what extent does the organization utilize an information security continuous monitoring (ISCM) strategy that addresses ISCM requirements and activities at each organizational tier and helps ensure an organizationwide approach to ISCM (NIST SP 800-37 (Rev. 2); NIST SP 800-137: Sections 3.1 and 3.6)?.

Consistently Implemented (Level 3)

Comments: The organization monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its ISCM strategy and makes updates, as appropriate. The organization ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format.

47 To what extent does the organization utilize ISCM policies and procedures to facilitate organization-wide, standardized processes in support of the ISCM strategy? ISCM policies and procedures address, at a minimum, the following areas: ongoing assessments and monitoring of security controls; collection of security related information required for metrics, assessments, and reporting; analyzing ISCM data, reporting findings, and reviewing and updating the ISCM strategy (NIST SP 800-53 REV. 4: CA-7, NISTIR 8011) (Note: The overall maturity level should take into consideration the maturity of question 49)?.

Consistently Implemented (Level 3)

Comments: The organization doesn't monitor and analyze qualitative and quantitative performance measures on the effectiveness of its ISCM policies and procedures and makes updates, as appropriate. The organization ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format.

48 To what extent have ISCM stakeholders and their roles, responsibilities, levels of authority, and dependencies been defined and communicated across the organization (NIST SP 800-53 REV. 4: CA-1; NIST SP 800-137; CSF: DE.DP-1; and FY 2019 CIO FISMA Metrics)?.

Ad Hoc (Level 1)

Comments: The organization has not defined and communicated the structures of its ISCM team, roles and responsibilities of ISCM stakeholders, and levels of authority and dependencies.

49 How mature are the organization's processes for performing ongoing assessments, granting system authorizations, and monitoring security controls (NIST SP 800- 137: Section 2.2; NIST SP 800- 53 REV. 4: CA-2, CA-6, and CA-7; NIST Supplemental Guidance on Ongoing Authorization; NIST SP 800-37 (Rev. 2); NISTIR 8011; OMB M-14-03; OMB M-19-03)

Consistently Implemented (Level 3)

Comments: The organization doesn't utilize the results of security control assessments and monitoring to maintain ongoing authorizations of information systems, including the maintenance of system security plans.

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)?

Consistently Implemented (Level 3)

Comments: The organization is not able to integrate metrics on the effectiveness of its ISCM program to deliver persistent situational awareness across the organization.

51.1 Please provide the assessed maturity level for the agency's Detect Function.

Consistently Implemented (Level 3)

Comments: Refer to the report draft.

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?

Refer to report draft.

Calculated Maturity Level - Consistently Implemented (Level 3)

Function 4: Respond - Incident Response

52 To what extent has the organization defined and implemented its incident response policies, procedures, plans, and strategies, as appropriate, to respond to cybersecurity events (NIST SP 800-53 REV. 4: IR-1; NIST SP 800-61 Rev. 2; NIST SP 800- 184; OMB M-17-25; OMB M- 17-09; FY 2018 CIO FISMA Metrics: 4.2; CSF: RS.RP-1; Presidential Policy Direction (PPD) 41)? (Note: The overall maturity level should take into consideration the maturity of questions 53 - 58).

Ad Hoc (Level 1)

Comments: The organization's incident response policies, procedures, plans, and strategies have not been defined and communicated.

53 To what extent have incident response team structures/models, stakeholders, and their roles, responsibilities, levels of authority, and dependencies been defined and communicated across the organization (NIST SP 800-53 REV. 4: IR-7; NIST SP 800-83; NIST SP 800-61 Rev. 2; OMB M-18-02; OMB M-16-04; FY 2019 CIO FISMA Metrics: Section 4; CSF: RS.CO-1; and US-CERT Federal Incident Notification Guidelines)?

Consistently Implemented (Level 3)

Comments: Resources (people, processes, and technology) are not allocated in a risk-based manner for stakeholders to effectively implement incident response activities.

Function 4: Respond - Incident Response

54 How mature are the organization's processes for incident detection and analysis? (NIST 800-53: IR-4 and IR-6; NIST SP 800-61 Rev. 2; OMB M-18-02; CSF: DE.AE-1, PR.DS-6, RS.AN-4, and PR.DS- 8; and US-CERT Incident Response Guidelines)

Consistently Implemented (Level 3)

Comments: The organization doesn't utilize profiling techniques to measure the characteristics of expected activities on its networks and systems so that it can more effectively detect security incidents.

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)

Comments: The organization doesn't manage and measure the impact of successful incidents and is not able to quickly mitigate related vulnerabilities on other systems.

56 To what extent does the organization ensure that incident response information is shared with individuals with significant security responsibilities and reported to external stakeholders in a timely manner (FISMA; OMB M-18-02; NIST SP 800-53 REV. 4: IR-6; US-CERT Incident Notification Guidelines; PPD-41; CSF: RS.CO-2 through 4; DHS Cyber Incident Reporting Unified Message)

Consistently Implemented (Level 3)

Comments: Incident response metrics are not used to measure and manage the timely reporting of incident information to organizational officials and external stakeholders.

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-18-02; PPD-41).

Consistently Implemented (Level 3)

Comments: The organization doesn't utilize Einstein 3 Accelerated to detect and proactively block cyber-attacks or prevent potential compromises.

Function 4: Respond - Incident Response

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

·Web application protections, such as web application firewalls

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

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

Malware detection, such as antivirus and antispam software technologies

·Information management, such as data loss prevention

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

Consistently Implemented (Level 3)

Comments: The organization doesn't use technologies for monitoring and analyzing qualitative and quantitative performance across the organization and is collecting, analyzing, and reporting data on the effectiveness of its technologies for performing incident response activities.

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

Consistently Implemented (Level 3)

Comments: Refer to the report draft.

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?

Refer to report draft.

Calculated Maturity Level - Consistently Implemented (Level 3)

Function 5: Recover - Contingency Planning

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

Ad Hoc (Level 1)

Comments: Roles and responsibilities of stakeholders have not been fully defined and communicated across the organization, including appropriate delegations of authority.

Function 5: Recover - Contingency Planning

61 To what extent has the organization defined and implemented its information system contingency planning program through policies, procedures, and strategies, as appropriate (Note: Assignment of an overall maturity level should take into consideration the maturity of questions 62-66) (NIST SP 800-34; NIST SP 800- 161; CSF: ID.BE-5, PR.IP-9, and ID.SC-5).

Ad Hoc (Level 1)

Comments: The organization has not defined its policies, procedures, and strategies, as appropriate, for information system contingency planning.

62 To what degree does the organization ensure that the results of business impact analyses are used to guide contingency planning efforts (NIST SP 800-53 REV. 4: CP-2; NIST SP 800-34, Rev. 1, 3.2; FIPS 199; FCD-1; OMB M-17- 09; FY 2019 CIO FISMA Metrics: 5.1; CSF:ID.RA-4)?

Consistently Implemented (Level 3)

63 To what extent does the organization ensure that information system contingency plans are developed, maintained, and integrated with other continuity plans (NIST SP 800- 53 REV. 4: CP-2; NIST SP 800- 34; FY 2019 CIO FISMA Metrics: 5.1; OMB M-19-03; CSF: PR.IP-9)?

Managed and Measurable (Level 4)

64 To what extent does the organization perform tests/exercises of its information system contingency planning processes (NIST SP 800-34; NIST SP 800-53 REV. 4: CP-3 and CP-4; FY 2019 CIO FISMA Metrics: 5.1; CSF: ID.SC-5 and CSF: PR.IP-10)?

Managed and Measurable (Level 4)

65 To what extent does the organization perform information system backup and storage, including use of alternate storage and processing sites, as appropriate (NIST SP 800-53 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 2019 CIO FISMA Metrics: 5.1.1; and NARA guidance on information systems security records)?

Consistently Implemented (Level 3)

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

Managed and Measurable (Level 4)

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

Managed and Measurable (Level 4)

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

Refer to report draft.

Calculated Maturity Level - Managed and Measurable (Level 4)

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.

·Do not include the names of specific independent auditors, these entities should be referred to as "independent assessor" or "independent auditor"

·The assessment of effectiveness should not include a list of ratings by NIST CSF Function-level, as these will already be included in the performance summary

Refer to the report draft.

APPENDIX A: Maturity Model Scoring

Function 1: Identify - Risk Management

Function	Count
Ad-Hoc	2
Defined	0
Consistently Implemented	0
Managed and Measurable	10
Optimized	0
Function Rating: Managed and Measurable (Level 4) Effective	

Function 2A: Protect - Configuration Management

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

Function 2B: Protect - Identity and Access Management

Function	Count
Ad-Hoc	5
Defined	0
Consistently Implemented	0
Managed and Measurable	2
Optimized	2
Function Rating: Ad Hoc (Level 1) Not Effective	

Function 2C: Protect - Data Protection and Privacy

Function	Count
Ad-Hoc	0
Defined	0
Consistently Implemented	2
Managed and Measurable	2
Optimized	1
Function Rating: Managed and Measurable (Level 4) Effective	

Function 2D: Protect - Security Training

Function	Count
Ad-Hoc	0
Defined	1
Consistently Implemented	0
Managed and Measurable	5
Optimized	0
Function Rating: Managed and Measurable (Level 4) Effective	

Function 3: Detect - ISCM

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

Function 4: Respond - Incident Response

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

Function 5: Recover - Contingency Planning

Function	Count
Ad-Hoc	2
Defined	0
Consistently Implemented	2
Managed and Measurable	3
Optimized	0
Function Rating: Managed and Measurable (Level 4) Effective	

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 & Access Management / Data Protection & Privacy / Security Training	Managed and Measurable (Level 4)	Managed and Measurable (Level 4)	
Function 3: Detect - ISCM	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	Refer to the report draft.
Function 4: Respond - Incident Response	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	Refer to the report draft.
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
James 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

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