Office of Inspector General

FISMA Evaluation

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

Fiscal Year 2016

Report No. ER-17-01

October 2016

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

DEMBO JONES
CERTIFIED PUBLIC ACCOUNTANTS & ADVISORS

OIG

Evaluation Report

The Federal Labor Relations Authority
Office of Inspector General

October 27, 2016

Carol Waller Pope
Chairman

Dembo, Jones, Healy, Pennington & Marshall, 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 Management Act (FISMA). This report was prepared in conjunction with the Inspector General (IG) and Dembo Jones. The weaknesses discussed in this report should be included in FLRA's Fiscal Year (FY) 2016 report to the Office of Management and Budget (OMB) and Congress.

Results in Brief

During our FY 2016 evaluation, we noted that FLRA has taken steps to improve the information security program. We also noted that FLRA does take information security weaknesses seriously. FLRA took action to remediate several weaknesses within specific control areas.

This year's FISMA testing included a follow up of all prior year recommendations. There were a total of 11 prior recommendations, of which 5 are still open. There are no new findings.

Background

On December 17, 2002, the President signed into law, 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

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

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

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

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 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 (SSPs), access control, the risk assessments, and the configuration management processes.

*****

Dembo Jones, P.C.

Dembo, Jones, Healy, Pennington & Marshall, P.C.

Rockville, Maryland
October 27, 2016

Appendix 1
Prior Year Recommendations

#	Year Initiated	Plan of Action and Milestones (POA&M)	Open / Closed
1	2009	*Develop a robust contingency planning program in accordance with NIST SP 800-53 Revision 3 Recommended Security Controls for Federal Information Systems.*	Closed
2	2011	*Dembo Jones obtained the latest Contingency Plan, as well as inquired about contingency testing in the event of a disaster. The following was noted:* 1. It was revealed that the latest Contingency Plan had not been signed or finalized.	Closed
3	2011	2. Furthermore, there have been no formalized tests of a contingency to be prepared in the event of a disaster.	Closed
4	2014	*Each of the SSPs have documentation to addresses the NIST 800-53 Revision 4 controls (e.g. account management, vulnerability scanning, and authenticator management), however, not all of the control objectives for each control are addressed. Due to the SSPs not containing the detail required in accordance with NIST 800-53 Revision 4, the controls were not assessed. Furthermore, because there was no continuous monitoring in terms of periodic testing, POA&Ms were not completed timely or not completed at all.* 1. Review all SSPs and ensure the documentation is clear and addresses each of the controls and all of their respective control objectives.	Closed
5	2014	2. All controls within NIST 800-53 Revision 4 for the systems' categorization should be used as a starting point for determining the assessments and implementation of a continuous monitoring program. Then, management should determine which of those controls are critical. Those critical controls should be assessed every year. The remainder of the controls should then be divided by three and then assessed over a three-year period, whereby 1/3 of the remaining controls are assessed each year. Ideally, the controls to be assessed each year should then be done on a quarterly basis by taking the annual set of controls and assessing ¼ each quarter. Upon completion of continuous monitoring, the agency should maintain metrics such as number of controls assessed on a monthly basis, number of deficiencies by family, etc.	Open
6	2014	3. Ensure any deficiencies as a result of the continuous monitoring assessments will be clearly and timely reported as a POA&M.	Open
7	2015	1. All vulnerabilities should be reviewed in terms of their risk classification (e.g. High, Medium, and Low). High vulnerabilities should be remediated within 1 business day and Medium vulnerabilities should be remediated within 3-5 business days. Documentation in these areas needs to be improved.	Open

#	Year Initiated	Plan of Action and Milestones (POA&M)	Open / Closed
8	2015	2. Any user that is terminated from the agency should have their access disabled within 5 business days. This needs to be documented to provide evidence that this is being done.	Open
9	2015	3. Incident Response prevention, detection and correction should be tested on an annual basis.	Closed
10	2015	4. All Users" access rights upon initiation should have their access rights reviewed, approved, and subsequently maintained for audit purposes.	Closed
11	2015	5. On an annual basis, all FLRA employees should have their access reviewed to ensure it still commensurate with their job functions. Consider having supervisors across the FLRA assist in this review of employees in their departments and provide the IT with the analysis.	Open

Appendix 2
Management Response

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

October 25, 2016

MEMORANDUM

TO: Dana Rooney-Fisher
Inspector General

FROM: Sarah Whittle-Spooner
Executive Director

SUBJECT: Follow-up Response and Action Plan Regarding Compliance with the Federal Information Security Management Act (FISMA) Fiscal Year (FY) 2016 Report

Thank you for the opportunity to provide a follow-up memo addressing the FISMA FY16 Report. Please find attached the Plan of Action and Milestones (POAM) that was developed in response to the Report. Plans have been developed for mitigating the vulnerabilities and are expected to be corrected by March 2017.

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

	Finding	Management Response	Corrective Timeline
1	Develop a robust contingency planning program in accordance with NIST Special Publication 800-53 Revision 3 Recommended Security Controls for Federal Information Systems . The organization: (i) does not test and/or exercise the contingency plan for the information system [Assignment: organization-defined frequency, at least annually] using [Assignment: organization-defined tests and/or exercises] to determine the plan's effectiveness and the organization's readiness to execute the plan; and (ii) does not review the contingency plan test/exercise results and does not initiate corrective actions The organization does not identify an alternate processing site and does not initiate necessary agreements to permit the resumption of information system operations for critical mission/business functions within [Assignment: organization-defined time period] when the primary processing capabilities are unavailable.	Completed and signed the Agency information technology continuity of operations plan (COOP).	Closed
2	Dembo Jones obtained the latest Contingency Plan, as well as inquired about contingency testing in the event of a disaster. The following was noted: 1. It was revealed that the latest Contingency Plan had not been signed or finalized.	See finding #1 - FLRA established an IT COOP plan and tested accordingly.	Closed
3	Continuous Monitoring / Security Plans Dembo Jones reviewed the System Security Plans (SSPs) and Security Controls Assessments (SCAs) for all systems in scope and noted the following: 1 - Each of the SSPs have documentation to addresses the NIST 800-53 Revision 4 controls (e.g. account management, vulnerability scanning, and authenticator management), however, not all of the control objectives for each control are addressed. 2 - Due to the SSPs not containing the detail required in accordance with NIST 800-53 Revision 4, the controls were not assessed.	IRMD Updated its SSP and took necessary steps to implement continuous monitoring.	Closed
4	Timely Remediation of Vulnerabilities Scan results were reviewed over a two week period to assess the timely remediation of any Medium and High vulnerabilities. Upon review of those scan results, we were unable to discern a total list of Low, Medium, and High risks, as well as how long it took to remediate those deficiencies. As a result, the condition is that deficiencies are not remediated in a timely manner.	The FLRA takes the remediation of vulnerabilities seriously and has committed to NIST 800-53, Revision 4, RA-5. While vulnerabilities were remediated in accordance with this guideline, as noted by the auditor, the documentation of said remediation was lacking. The FLRA intends to implement a more stringent documentation policy of all steps taken to remediate vulnerabilities in a timely manner.	Spring 2017
5	Personnel Termination Upon review of the users that were terminated from the agency, it was not discernable how many days it took to remove the users' access after their respective termination date.	Upon termination, the FLRA takes many steps to ensure account access and Agency owned assets are dealt with appropriately. The FLRA will update its policy and documentation showing the actions taken.	Spring 2017
6	Upon review of Incident Response planning and testing; the following was noted: There is no testing of the current incidence response environment There is no training provided to the IT staff with respect to preparing for and managing incidents	The FLRA finalized its Incident Response Plan and all IT personnel participated in all aspects of Incident Response planning, testing, and training as coordinated by the FLRA's Information Systems Security Manager.	Closed
7	Access Authorization Upon review of a sample of a set of users for assessing their access authorizations; the following was noted: Access authorization forms (paper or electronic) are not being maintained to ensure that users' rights are commensurate with what was approved An annual recertification of users' access rights are not being performed.	While the FLRA did perform the necessary audits and permission confirmation practices, the processes were not properly documented. This made it difficult for the auditor to confirm. As with the above findings, the Information Systems Security Manager will document the appropriate steps for these activities in a verifiable manner.	Spring 2017
8	All controls within NIST 800-53 Revision 4 for the systems' categorization should be used as a starting point for determining the assessments and implementation of a continuous monitoring program. Then, management should determine which of those controls are critical. Those critical controls should be assessed every year. The remainder of the controls should then divided by three and then assessed over a three year period, whereby 1/3 of the remaining controls are assessed each year. Ideally, the controls to assessed each year should then done on a quarterly basis by taking the annual set of controls and assessing 1/4 each quarter. Upon completion of continuous monitoring, the agency should maintain metrics such as number of controls assessed on a monthly basis, number of deficiencies by family, etc.	With the documents produced by our consultant, Telos, and the work performed by IRMD's intern, it's now simply up to IRMD to execute the continuous monitoring plan for FY 2017. IRMD will schedule quarterly review of the NIST 800-53 Revision 4 controls, ensuring all controls are reviewed over a three year period.	Spring 2017
9	Ensure any deficiencies as a result of the continuous monitoring assessments will be clearly and timely reported as POA&M.	IRMD will address this need in combination with the execution of the continuous monitoring plan.	Spring 2017

Appendix 3
OIG Responses Report in Cyberscope

For Official Use Only

Inspector General

Section Report

2016
Annual FISMA
Report

Federal Labor Relations Authority

For Official Use Only

Section 0: Overall

0.1 Please provide an overall narrative assessment of the agency's information security program. 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 this response to conform with the grammatical and narrative structure of the Annual Report.

This agency has a robust security program with regular scanning, as well as a host of both physical and logical security controls.

Section 1: Identify

Risk Management (Identify)

1.1	Has the organization established a risk management program that includes comprehensive agency policies and procedures consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? **Met**	**Defined**
1.1.1	Identifies and maintains an up-to-date system inventory, including organization- and contractor-operated systems, hosting environments, and systems residing in the public, hybrid, or private cloud. (2016 CIO FISMA Metrics, 1.1; NIST Cybersecurity Framework (CF) ID.AM.1, NIST 800-53: PM-5) **Met**	**Defined**
1.1.2	Develops a risk management function that is demonstrated through the development, implementation, and maintenance of a comprehensive governance structure and organization-wide risk management strategy as described in NIST SP 800-37, Rev. 1. (NIST SP 800-39) **Met**	**Consistently Implemented**
1.1.3	Incorporates mission and business process-related risks into risk-based decisions at the organizational perspective, as described in NIST SP 800-37, Rev. 1. (NIST SP 800-39) **Met**	**Consistently Implemented**
1.1.4	Conducts information system level risk assessments that integrate risk decisions from the organizational and mission/business process perspectives and take into account threats, vulnerabilities, likelihood, impact, and risks from external parties and common control providers. (NIST SP 800-37, Rev. 1, NIST SP 800-39, NIST SP 800-53: RA-3) **Met**	**Consistently Implemented**
1.1.5	Provides timely communication of specific risks at the information system, mission/business, and organization-level to appropriate levels of the organization. **Met**	**Managed and Measureable**
1.1.6	Performs comprehensive assessments to categorize information systems in accordance with Federal standards and applicable guidance. (FIPS 199, FIPS 200, FISMA, Cybersecurity Sprint, OMB M-16-04, President's Management Council (PMC) cybersecurity assessments) **Met**	**Consistently Implemented**

Section 1: Identify

1.1.7	Selects an appropriately tailored set of baseline security controls based on mission/business requirements and policies and develops procedures to employ controls within the information system and its environment of operation. **Met**	**Defined**
1.1.8	Implements the tailored set of baseline security controls as described in 1.1.7. **Met**	**Consistently Implemented**
1.1.9	Identifies and manages risks with system interconnections, including through authorizing system interconnections, documenting interface characteristics and security requirements, and maintaining interconnection security agreements. (NIST SP 800-53: CA-3) **Met**	**Managed and Measureable**
1.1.10	Continuously assesses the security controls, including hybrid and shared controls, using appropriate assessment procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. **Not Met**	**Consistently Implemented**
	Comments: The controls from NIST 800-53 are assessed, however they were not assessed on a quarterly basis covering all of the controls over a 3 year period.	
1.1.11	Maintains ongoing information system authorizations based on a determination of the risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation of the information system and the decision that this risk is acceptable (OMB M-14-03, NIST Supplemental Guidance on Ongoing Authorization). **Met**	**Managed and Measureable**
1.1.12	Security authorization package contains system security plan, security assessment report, and POA&M that are prepared and maintained in accordance with government policies. (SP 800-18, SP 800-37) **Met**	**Managed and Measureable**
1.1.13	POA&Ms are maintained and reviewed to ensure they are effective for correcting security weaknesses. **Met**	**Consistently Implemented**

Section 1: Identify

1.1.14	Centrally tracks, maintains, and independently reviews/validates POA&M activities at least quarterly. (NIST SP 800-53 CA-5; OMB M-04-25) **Met**	**Managed and Measureable**
1.1.15	Prescribes the active involvement of information system owners and common control providers, chief information officers, senior information security officers, authorizing officials, and other roles as applicable in the ongoing management of information-system-related security risks. **Met**	**Managed and Measureable**
1.1.16	Implemented an insider threat detection and prevention program, including the development of comprehensive policies, procedures, guidance, and governance structures, in accordance with Executive Order 13587 and the National Insider Threat Policy. (PMC; NIST SP 800-53: PM-12) **Met**	**Consistently Implemented**
1.1.17	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. Based on all testing performed, is the Risk Management program effective? **Effective**	

Contractor Systems (Identify)

1.2	Has the organization established a program to oversee systems operated on its behalf by contractors or other entities, including other government agencies, managed hosting environments, and systems and services residing in a cloud external to the organization that is inclusive of policies and procedures consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? **Met**	**Defined**
1.2.1	Establishes and implements a process to ensure that contracts/statements of work/solicitations for systems and services, include appropriate information security and privacy requirements and material disclosures, FAR clauses, and clauses on protection, detection, and reporting of information. (FAR Case 2007-004, Common Security Configurations, FAR Sections 24.104, 39.101, 39.105, 39.106, 52.239-1; PMC, 2016 CIO Metrics 1.8, NIST 800-53, SA-4 FedRAMP standard contract clauses; Cloud Computing Contract Best Practices) **Met**	**Consistently Implemented**

Section 1: Identify

1.2.2	Specifies within appropriate agreements how information security performance is measured, reported, and monitored on contractor- or other entity-operated systems. (CIO and CAO Council Best Practices Guide for Acquiring IT as a Service, NIST SP 800-35) **Met**	**Consistently Implemented**
1.2.3	Obtains sufficient assurance that the security controls of systems operated on the organization's behalf by contractors or other entities and services provided on the organization's behalf meet FISMA requirements, OMB policy, and applicable NIST guidelines. (NIST SP 800-53: CA-2, SA-9) **Met**	**Consistently Implemented**
1.2.4	Provide any additional information on the effectiveness (positive or negative) of the organization's Contractor Systems Program that was not noted in the questions above. Based on all testing performed, is the Contractor Systems Program effective? **Effective**	

Level	Score	Possible Score
LEVEL 3: Consistently Implemented	13	20

Section 2: Protect

Configuration Management (Protect)

2.1	Has the organization established a configuration management program that is inclusive of comprehensive agency policies and procedures consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? **Met**	**Defined**
2.1.1	Develops and maintains an up-to-date inventory of the hardware assets (i.e., endpoints, mobile assets, network devices, input/output assets, and SMART/NEST devices) connected to the organization's network with the detailed information necessary for tracking and reporting. (NIST CF ID.AM-1; 2016 CIO FISMA Metrics 1.5, 3.17; NIST 800-53: CM-8) **Met**	**Defined**
2.1.2	Develops and maintains an up-to-date inventory of software platforms and applications used within the organization and with the detailed information necessary for tracking and reporting. (NIST 800-53: CM-8, NIST CF ID.AM-2) **Met**	**Defined**
2.1.3	Implements baseline configurations for IT systems that are developed and maintained in accordance with documented procedures. (NIST SP 800-53: CM-2; NIST CF PR.IP-1) **Met**	**Consistently Implemented**
2.1.4	Implements and maintains standard security settings (also referred to as security configuration checklists or hardening guides) for IT systems in accordance with documented procedures. (NIST SP 800-53: CM-6; CIO 2016 FISMA Metrics, 2.3) **Met**	**Consistently Implemented**
2.1.5	Assesses configuration change control processes, including processes to manage configuration deviations across the enterprise that are implemented and maintained. (NIST SP 800-53: CM-3, NIST CF PR.IP-3) **Met**	**Managed and Measureable**
2.1.6	Identifies and documents deviations from configuration settings. Acceptable deviations are approved with business justification and risk acceptance. Where appropriate, automated means that enforce and redeploy configuration settings to systems at regularly scheduled intervals are deployed, while evidence of deviations is also maintained. (NIST SP 800-53: CM-6, Center for Internet Security Controls (CIS) 3.7) **Met**	**Managed and Measureable**

Section 2: Protect

2.1.7	Implemented SCAP certified software assessing (scanning) capabilities against all systems on the network to assess both code-based and configuration-based vulnerabilities in accordance with risk management decisions. (NIST SP 800-53: RA-5, SI- 2; CIO 2016 FISMA Metrics 2 2, CIS 4 1) **Met**	**Managed and Measureable**
2.1.8	Remediates configuration-related vulnerabilities, including scan findings, in a timely manner as specified in organization policy or standards. (NIST 800-53: CM-4, CM-6, RA-5, SI-2) **Met**	**Consistently Implemented**
2.1.9	Develops and implements a patch management process in accordance with organization policy or standards, including timely and secure installation of software patches. (NIST SP 800-53: CM-3, SI-2, OMB M-16-04, DHS Binding Operational Directive 15-01) **Met**	**Managed and Measureable**
2.1.10	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. Based on all testing performed, is the Configuration Management Program effective? **Effective**	

Identity and Access Management (Protect)

2.2	Has the organization established an identity and access management program, including policies and procedures consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? **Met**	**Defined**
2.2.1	Ensures that individuals requiring access to organizational information and information systems sign appropriate access agreements, participate in required training prior to being granted access, and recertify access agreements on a predetermined interval. (NIST 800-53: PL-4, PS-6) **Met**	**Consistently Implemented**
2.2.2	Ensures that all users are only granted access based on least privilege and separation-of-duties principles. **Not Met**	**Consistently Implemented**

Comments: Users access rights were not reviewed on an annual basis.

Section 2: Protect

2.2.3	Distinguishes hardware assets that have user accounts (e g , desktops, laptops, servers) from those without user accounts (e.g. networking devices, such as load balancers and intrusion detection/prevention systems, and other input/output devices such as faxes and IP phones). **Met**	**Consistently Implemented**
2.2.4	Implements PIV for physical access in accordance with government policies. (HSPD 12, FIPS 201, OMB M-05-24, OMB M-07-06, OMB M-08-01, OMB M-11-11) **Met**	**Consistently Implemented**
2.2.5	Implements PIV or a NIST Level of Assurance (LOA) 4 credential for logical access by all privileged users (system, network, database administrators, and others responsible for system/application control, monitoring, or administration functions). (Cybersecurity Sprint, OMB M-16-04, PMC, 2016 CIO FISMA Metrics 2 5 1) **Met**	**Consistently Implemented**
2.2.6	Enforces PIV or a NIST LOA 4 credential for logical access for at least 85% of non-privileged users. (Cybersecurity Sprint, OMB M-16-04, PMC, 2016 CIO FISMA Metrics 2 4.1) **Met**	**Consistently Implemented**
2.2.7	Tracks and controls the use of administrative privileges and ensures that these privileges are periodically reviewed and adjusted in accordance with organizationally defined timeframes. (2016 CIO FISMA Metrics 2.9, 2.10; OMB M-16-04, CIS 5.2) **Met**	**Managed and Measureable**
2.2.8	Ensures that accounts are terminated or deactivated once access is no longer required or after a period of inactivity, according to organizational policy. **Not Met** **Comments:** There were users that were terminated where their access was not removed within a timely manner.	**Managed and Measureable**
2.2.9	Identifies, limits, and controls the use of shared accounts. (NIST SP 800-53: AC-2) **Met**	**Consistently Implemented**

Section 2: Protect

2.2.10	All users are uniquely identified and authenticated for remote access using Strong Authentication (multi-factor), including PIV. (NIST SP 800-46, Section 4 2, Section 5.1, NIST SP 800-63) **Met**	**Consistently Implemented**
2.2.11	Protects against and detects unauthorized remote access connections or subversion of authorized remote access connections, including through remote scanning of host devices. (CIS 12.7, 12 8, FY 2016 CIO FISMA metrics 2.17.3, 2.17.4, 3.11, 3.11.1) **Met**	**Consistently Implemented**
2.2.12	Remote access sessions are timed-out after 30 minutes of inactivity, requiring user re-authentication, consistent with OMB M-07-16 **Met**	**Managed and Measureable**
2.2.13	Enforces a limit of consecutive invalid remote access logon attempts and automatically locks the account or delays the next logon prompt. (NIST 800-53: AC-7) **Met**	**Consistently Implemented**
2.2.14	Implements a risk-based approach to ensure that all agency public websites and services are accessible through a secure connection through the use and enforcement of https and strict transport security. (OMB M-15-13) **Met**	**Consistently Implemented**
2.2.15	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. Based on all testing performed is the Identity and Access Management Program effective? **Effective**	

Security and Privacy Training (Protect)

2.3	Has the organization established a security and privacy awareness and training program, including comprehensive agency policies and procedures consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? **Met**	**Defined**

Section 2: Protect

2.3.1	Develops training material for security and privacy awareness training containing appropriate content for the organization, including anti-phishing, malware defense, social engineering, and insider threat topics. (NIST SP 800-50, 800-53: AR-5, OMB M-15-01, 2016 CIO Metrics, PMC, National Insider Threat Policy (NITP)) **Met**	**Consistently Implemented**
2.3.2	Evaluates the skills of individuals with significant security and privacy responsibilities and provides additional security and privacy training content or implements human capital strategies to close identified gaps. (NIST SP 800-50) **Met**	**Consistently Implemented**
2.3.3	Identifies and tracks status of security and privacy awareness training for all information system users (including employees, contractors, and other organization users) requiring security awareness training with appropriate internal processes to detect and correct deficiencies. (NIST 800-53: AT-2) **Met**	**Consistently Implemented**
2.3.4	Identifies and tracks status of specialized security and privacy training for all personnel (including employees, contractors, and other organization users) with significant information security and privacy responsibilities requiring specialized training **Met**	**Consistently Implemented**
2.3.5	Measures the effectiveness of its security and privacy awareness and training programs, including through social engineering and phishing exercises. (PMC, 2016 CIO FISMA Metrics 2.19, NIST SP 800-50, NIST SP 800-55) **Met**	**Managed and Measureable**
2.3.6	Provide any additional information on the effectiveness (positive or negative) of the organization's Security and Privacy Training Program that was not noted in the questions above. Based on all testing performed is the Security and Privacy Training Program effective? **Effective**	

Level	Score	Possible Score
LEVEL 3: Consistently Implemented	13	20

Section 3: Detect

Level 1

Definition

3.1.1 ISCM program is not formalized and ISCM activities are performed in a reactive manner resulting in an ad hoc program that does not meet Level 2 requirements for a defined program consistent with NIST SP 800-53, SP 800-137, OMB M-14-03, and the CIO ISCM CONOPS.

People

3.1.1.1 ISCM stakeholders and their responsibilities have not been fully defined and communicated across the organization. **Ad Hoc**
Met

3.1.1.2 The organization has not performed an assessment of the skills, knowledge, and resources needed to effectively implement an ISCM program. Key personnel do not possess knowledge, skills, and abilities to successfully implement an effective ISCM program. **Ad Hoc**
Met

3.1.1.3 The organization has not defined how ISCM information will be shared with individuals with significant security responsibilities and used to make risk based decisions. **Ad Hoc**
Met

3.1.1.4 The organization has not defined how it will integrate ISCM activities with organizational risk tolerance, the threat environment, and business/mission requirements. **Ad Hoc**
Met

Processes

3.1.1.5 ISCM processes have not been fully defined and are performed in an ad-hoc, reactive manner for the following areas: ongoing assessments and monitoring of security controls; performing hardware asset management, software asset management, configuration setting management, and common vulnerability management; collecting security related information required for metrics, assessments, and reporting; analyzing ISCM data, reporting findings, and determining the appropriate risk responses; and reviewing and updating the ISCM program. **Ad Hoc**
Met

3.1.1.6 ISCM results vary depending on who performs the activity, when it is performed, and the methods and tools used. **Ad Hoc**
Met

Section 3: Detect

3.1.1.7	The organization has not identified and defined the qualitative and quantitative performance measures that will be used to assess the effectiveness of its ISCM program, achieve situational awareness, and control ongoing risk. **Met**	**Ad Hoc**
3.1.1.8	The organization has not defined its processes for collecting and considering lessons learned to improve ISCM processes. **Met**	**Ad Hoc**

Technology

3.1.1.9	The organization has not identified and defined the ISCM technologies needed in one or more of the following automation areas and relies on manual/procedural methods in instances where automation would be more effective. Use of ISCM technologies in the following areas is ad-hoc. - Patch management - License management - Information management - Software assurance - Vulnerability management - Event management - Malware detection - Asset management - Configuration management - Network management - Incident management **Met**	**Ad Hoc**
3.1.1.10	The organization has not defined how it will use automation to produce an accurate point-in-time inventory of the authorized and unauthorized devices and software on its network and the security configuration of these devices and software. **Met**	**Ad Hoc**

Level 2

Definition

Section 3: Detect

3.2.1 The organization has formalized its ISCM program through the development of comprehensive ISCM policies, procedures, and strategies consistent with NIST SP 800-53, SP 800-137, OMB M-14-03, and the CIO ISCM CONOPS. However, ISCM policies, procedures, and strategies are not consistently implemented organization-wide.

People

3.2.1.1 ISCM stakeholders and their responsibilities have been defined and communicated across the organization. However, stakeholders may not have adequate resources (people, processes, and technology) to effectively implement ISCM activities. **Defined**

Met

3.2.1.2 The organization has performed an assessment of the skills, knowledge, and resources needed to effectively implement an ISCM program. In addition, the organization has developed a plan for closing any gaps identified. However, key personnel may still lack the knowledge, skills, and abilities to successfully implement an effective ISCM program. **Defined**

Met

3.2.1.3 The organization has defined how ISCM information will be shared with individuals with significant security responsibilities and used to make risk-based decisions. However, ISCM information is not always shared with individuals with significant security responsibilities in a timely manner with which to make risk-based decisions. **Defined**

Met

3.2.1.4 The organization has defined how it will integrate ISCM activities with organizational risk tolerance, the threat environment, and business/mission requirements. However, ISCM activities are not consistently integrated with the organization's risk management program. **Defined**

Met

Processes

3.2.1.5 ISCM processes have been fully defined for the following areas: ongoing assessments and monitoring of security controls; performing hardware asset management, software asset management, configuration setting management, and common vulnerability management; collecting security related information required for metrics, assessments, and reporting; analyzing ISCM data, reporting findings, and determining the appropriate risk responses; and reviewing and updating the ISCM program. However, these processes are inconsistently implemented across the organization. **Defined**

Met

Section 3: Detect

3.2.1.6	ISCM results vary depending on who performs the activity, when it is performed, and the methods and tools used. **Met**	**Defined**
3.2.1.7	The organization has identified and defined the performance measures and requirements that will be used to assess the effectiveness of its ISCM program, achieve situational awareness, and control ongoing risk. However, these measures are not consistently collected, analyzed, and used across the organization. **Met**	**Defined**
3.2.1.8	The organization has a defined process for capturing lessons learned on the effectiveness of its ISCM program and making necessary improvements However, lessons learned are not consistently shared across the organization and used to make timely improvements to the ISCM program. **Met**	**Defined**

Technology

3.2.1.9	The organization has identified and fully defined the ISCM technologies it plans to utilize in the following automation areas. In addition, the organization has developed a plan for implementing ISCM technologies in these areas: patch management, license management, information management, software assurance, vulnerability management, event management, malware detection, asset management, configuration management, network management, and incident management. However, the organization has not fully implemented technology is these automation areas and continues to rely on manual/procedural methods in instances where automation would be more effective. In addition, while automated tools are implemented to support some ISCM activities, the tools may not be interoperable. **Met**	**Defined**
3.2.1.10	The organization has defined how it will use automation to produce an accurate point-in-time inventory of the authorized and unauthorized devices and software on its network and the security configuration of these devices and software. However, the organization does not consistently implement the technologies that will enable it to manage an accurate point-in-time inventory of the authorized and unauthorized devices and software on its network and the security configuration of these devices and software. **Met**	**Defined**

Level 3

Definition

Section 3: Detect

3.3.1 In addition to the formalization and definition of its ISCM program (Level 2), the organization consistently implements its ISCM program across the agency. However, qualitative and quantitative measures and data on the effectiveness of the ISCM program across the organization are not captured and utilized to make risk-based decisions, consistent with NIST SP 800-53, SP 800-137, OMB M-14-03, and the CIO ISCM CONOPS.

People

3.3.1.1	ISCM stakeholders and their responsibilities have been identified and communicated across the organization, and stakeholders have adequate resources (people, processes, and technology) to effectively implement ISCM activities. **Met**	**Consistently Implemented**
3.3.1.2	The organization has fully implemented its plans to close any gapes in skills, knowledge, and resources required to successfully implement an ISCM program. Personnel possess the required knowledge, skills, and abilities to effectively implement the organization's ISCM program. **Met**	**Consistently Implemented**
3.3.1.3	ISCM information is shared with individuals with significant security responsibilities in a consistent and timely manner with which to make risk-based decisions and support ongoing system authorizations. **Met**	**Consistently Implemented**
3.3.1.4	ISCM activities are fully integrated with organizational risk tolerance, the threat environment, and business/mission requirements. **Met**	**Consistently Implemented**

Processes

3.3.1.5	ISCM processes are consistently performed across the organization in the following areas: ongoing assessments and monitoring of security controls; performing hardware asset management, software asset management, configuration setting management, and common vulnerability management; collecting security related information required for metrics, assessments, and reporting; analyzing ISCM data, reporting findings, and determining the appropriate risk responses, and reviewing and updating the ISCM program. **Met**	**Consistently Implemented**
3.3.1.6	The rigor, intensity, scope, and results of ISCM activities are comparable and predictable across the organization. **Met**	**Consistently Implemented**

Section 3: Detect

3.3.1.7	The organization is consistently capturing qualitative and quantitative performance measures on the performance of its ISCM program in accordance with established requirements for data collection, storage, analysis, retrieval, and reporting. ISCM measures provide information on the effectiveness of ISCM processes and activities. **Met**	**Consistently Implemented**
3.3.1.8	The organization is consistently capturing and sharing lessons learned on the effectiveness of ISCM processes and activities. Lessons learned serve as a key input to making regular updates to ISCM processes. **Met**	**Consistently Implemented**
3.3.1.9	The organization has consistently implemented its defined technologies in all of the following ISCM automation areas. ISCM tools are interoperable to the extent practicable - Patch management - License management - Information management - Software assurance - Vulnerability management - Event management - Malware detection - Asset management - Configuration management - Network management - Incident management **Met**	**Consistently Implemented**

Technology

3.3.1.10	The organization can produce an accurate point-in-time inventory of the authorized and unauthorized devices and software on its network and the security configuration of these devices and software. **Met**	**Consistently Implemented**

Level 4

Definition

Section 3: Detect

3.4.1 In addition to being consistently implemented (Level 3), ISCM activities are repeatable and metrics are used to measure and manage the implementation of the ISCM program, achieve situational awareness, control ongoing risk, and perform ongoing system authorizations.

People

3.4.1.1	The organization's staff is consistently implementing, monitoring, and analyzing qualitative and quantitative performance measures across the organization and is collecting, analyzing, and reporting data on the effectiveness of the organization's ISCM program. **Met**	**Managed and Measureable**
3.4.1.2	Skilled personnel have been hired and/or existing staff trained to develop the appropriate metrics to measure the success of the ISCM program. **Met**	**Managed and Measureable**
3.4.1.3	Staff are assigned responsibilities for developing and monitoring ISCM metrics, as well as updating and revising metrics as needed based on organization risk tolerance, the threat environment, business/mission requirements, and the results of the ISCM program. **Met**	**Managed and Measureable**

Processes

3.4.1.4	The organization has processes for consistently implementing, monitoring, and analyzing qualitative and quantitative performance measures across the organization and is collecting, analyzing, and reporting data on the effectiveness of its processes for performing ISCM. **Met**	**Managed and Measureable**
3.4.1.5	Data supporting ISCM metrics are obtained accurately, consistently, and in a reproducible format. **Met**	**Managed and Measureable**
3.4.1.6	The organization is able to integrate metrics on the effectiveness of its ISCM program to deliver persistent situational awareness across the organization, explain the environment from both a threat/vulnerability and risk/impact perspective, and cover mission areas of operations and security domains. **Met**	**Managed and Measureable**

Section 3: Detect

3.4.1.7	The organization uses its ISCM metrics for determining risk response actions including risk acceptance, avoidance/rejection, or transfer. **Met**	**Managed and Measureable**
3.4.1.8	ISCM metrics are reported to the organizational officials charged with correlating and analyzing the metrics in ways that are relevant for risk management activities. **Met**	**Managed and Measureable**
3.4.1.9	ISCM is used to maintain ongoing authorizations of information systems and the environments in which those systems operate, including common controls and keep required system information and data (i.e., System Security Plan Risk Assessment Report, Security Assessment Report, and POA&M) up to date on an ongoing basis. **Met**	**Managed and Measureable**

Technology

3.4.1.10	The organization uses technologies for consistently implementing, 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 ISCM. **Met**	**Managed and Measureable**
3.4.1.11	The organization's ISCM performance measures include data on the implementation of its ISCM program for all sections of the network from the implementation of technologies that provide standard calculations, comparisons, and presentations **Met**	**Managed and Measureable**
3.4.1.12	The organization utilizes a SIEM tool to collect, maintain, monitor, and analyze IT security information, achieve situational awareness, and manage risk **Met**	**Managed and Measureable**

Level 5

Definition

3.5.1 In addition to being managed and measurable (Level 4), the organization's ISCM program is institutionalized, repeatable, self-regenerating, and updated in a near real-time basis based on changes in business/mission requirements and a changing threat and technology landscape.

People

Section 3: Detect

3.5.1.1 The organization's assigned personnel collectively possess a high skill level to perform and update ISCM activities on a near real-time basis to make any changes needed to address ISCM results based on organization risk tolerance, the threat environment, and business/mission requirements. **Optimized**

Met

Processes

3.5.1.2 The organization has institutionalized a process of continuous improvement incorporating advanced cybersecurity and practices. **Optimized**

Met

3.5.1.3 On a near real-time basis, the organization actively adapts its ISCM program to a changing cybersecurity landscape and responds to evolving and sophisticated threats in a timely manner. **Optimized**

Not Met

Comments: Scans are performed weekly however the vulnerabilities were not remediated timely.

3.5.1.4 The ISCM program is fully integrated with strategic planning, enterprise architecture and capital planning and investment control processes, and other mission/business areas, as appropriate. **Optimized**

Met

3.5.1.5 The ISCM program achieves cost-effective IT security objectives and goals and influences decision making that is based on cost, risk, and mission impact. **Optimized**

Met

Technology

3.5.1.6 The organization has institutionalized the implementation of advanced cybersecurity technologies in near real-time. **Optimized**

Met

3.5.1.7 The organization has institutionalized the use of advanced technologies for analysis of trends and performance against benchmarks to continuously improve its ISCM program. **Optimized**

Met

Level	Score	Possible Score
LEVEL 4: Managed and Measureable	18	20

Section 4: Respond

Level 1

Definition

4.1.1 Incident response program is not formalized and incident response activities are performed in a reactive manner resulting in an ad-hoc program that does not meet Level 2 requirements for a defined program consistent with FISMA (including guidance from NIST SP 800-83, NIST SP 800-61 Rev. 2, NIST SP 800-53, OMB M-16-03, OMB M-16-04, and US-CERT Federal Incident Notification Guidelines).

People

4.1.1.1 Incident response team structures/models, stakeholders, and their roles, responsibilities, levels of authority, and dependencies have not been fully defined and communicated across the organization, including the designation of a principal security operations center or equivalent organization that is accountable to agency leadership, DHS, and OMB for all incident response activities. **Ad Hoc**

Met

4.1.1.2 The organization has not performed an assessment of the skills, knowledge, and resources needed to effectively implement an incident response program. Key personnel do not possess the knowledge, skills, and abilities to successfully implement an effective incident response program. **Ad Hoc**

Met

4.1.1.3 The organization has not defined a common threat vector taxonomy and defined how incident response information will be shared with individuals with significant security responsibilities and other stakeholders, and used to make timely, risk-based decisions. **Ad Hoc**

Met

4.1.1.4 The organization has not defined how it will integrate incident response activities with organizational risk management, continuous monitoring, continuity of operations, and other mission/business areas, as appropriate. **Ad Hoc**

Met

Processes

4.1.1.5 Incident response processes have not been fully defined and are performed in an ad-hoc, reactive manner for the following areas: incident response planning, incident response training and testing; incident detection and analysis; incident containment, eradication, and recovery; incident coordination, information sharing, and reporting to internal and external stakeholders using standard data elements and impact classifications within timeframes established by US-CERT. **Ad Hoc**

Met

Section 4: Respond

4.1.1.6	The organization has not fully defined how it will collaborate with DHS and other parties, as appropriate, to provide on-site, technical assistance/surge resources/special capabilities for quickly responding to incidents. **Met**	**Ad Hoc**
4.1.1.7	The organization has not identified and defined the qualitative and quantitative performance measures that will be used to assess the effectiveness of its incident response program, perform trend analysis, achieve situational awareness, and control ongoing risk. **Met**	**Ad Hoc**
4.1.1.8	The organization has not defined its processes for collecting and considering lessons learned and incident data to improve security controls and incident response processes. **Met**	**Ad Hoc**
Technology		
4.1.1.9	The organization has not identified and defined the incident response technologies needed in one or more of the following areas and relies on manual/procedural methods in instances where automation would be more effective. Use of incident response technologies in the following areas is ad-hoc. - 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 anti-virus and antispam software technologies - Information management, such as data loss prevention - File integrity and endpoint and server security tools **Met**	**Ad Hoc**
4.1.1.10	The organization has not defined how it will meet the defined Trusted Internet Connection (TIC) security controls and ensure that all agency traffic, including mobile and cloud, are routed through defined access points, as appropriate. **Met**	**Ad Hoc**
4.1.1.11	The organization has not defined how it plans to utilize DHS' Einstein program for intrusion detection/prevention capabilities for traffic entering and leaving the organization's networks. **Met**	**Ad Hoc**

Section 4: Respond

4.1.1.12 The organization has not defined how it plans to utilize technology to develop and maintain a baseline of network operations and expected data flows for users and systems. **Ad Hoc**

Met

Level 2

Definition

4.2.1 The organizational has formalized its incident response program through the development of comprehensive incident response policies, plans, and procedures consistent with FISMA (including guidance from NIST SP 800-83, NIST SP 800-61 Rev. 2, NIST SP 800-53, OMB M-16-03, OMB M-16-04, and US-CERT Federal Incident Notification Guidelines). However, incident response policies, plans, and procedures are not consistently implemented organization-wide.

People

4.2.1.1 Incident response team structures/models, stakeholders, and their roles, responsibilities, levels of authority, and dependencies have been fully defined and communicated across the organization, including the designation of a principal security operations center or equivalent organization that is accountable to agency leadership, DHS, and OMB for all incident response activities. However, stakeholders may not have adequate resources (people, processes, and technology) to effectively implement incident response activities. Further, the organization has not verified roles and responsibilities as part of incident response testing. **Defined**

Met

4.2.1.2 The organization has performed an assessment of the skills, knowledge, and resources needed to effectively implement an incident response program. In addition, the organization has developed a plan for closing any gaps identified. However, key personnel may still lack the knowledge, skills, and abilities to successfully implement an effective incident response program. **Defined**

Met

4.2.1.3 The organization has defined a common threat vector taxonomy and defined how incident response information will be shared with individuals with significant security responsibilities and other stakeholders, and used to make timely, risk-based decisions. However, the organization does not consistently utilize its threat vector taxonomy and incident response information is not always shared with individuals with significant security responsibilities and other stakeholders in a timely manner. **Defined**

Met

Section 4: Respond

4.2.1.4	The organization has defined how it will integrate incident response activities with organizational risk management, continuous monitoring, continuity of operations, and other mission/business areas, as appropriate. However, incident response activities are not consistently integrated with these areas. **Met**	**Defined**

Processes

4.2.1.5	Incident response processes have been fully defined for the following areas: incident response planning, incident response training and testing; incident detection and analysis; incident containment, eradication, and recovery; incident coordination, information sharing, and reporting using standard data elements and impact classifications within timeframes established by US-CERT. However, these processes are inconsistently implemented across the organization. **Met**	**Defined**
4.2.1.6	The organization has fully defined, but not consistently implemented, its processes to collaborate with DHS and other parties as appropriate, to provide on-site, technical assistance/surge resources/special capabilities for quickly responding to incidents. **Met**	**Defined**
4.2.1.7	The organization has identified and defined the qualitative and quantitative performance measures that will be used to assess the effectiveness of its incident response program, perform trend analysis, achieve situational awareness, and control ongoing risk. However, these measures are not consistently collected, analyzed, and used across the organization. **Met**	**Defined**
4.2.1.8	The organization has defined its processes for collecting and considering lessons learned and incident data to improve security controls and incident response processes. However, lessons learned are not consistently captured and shared across the organization and used to make timely improvements to security controls and the incident response program. **Met**	**Defined**

Technology

Section 4: Respond

4.2.1.9	The organization has identified and fully defined the incident response technologies it plans to utilize in the following areas: - 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. However, the organization has not ensured that security and event data are aggregated and correlated from all relevant sources and sensors. - Malware detection such as Anti-virus and antispam software technologies - Information management such as data loss prevention - File integrity and endpoint and server security tools However, the organization has not fully implemented technologies in these areas and continues to rely on manual/procedural methods in instances where automation would be more effective. In addition, while tools are implemented to support some incident response activities, the tools are not interoperable to the extent practicable, do not cover all components of the organization's network, and/or have not been configured to collect and retain relevant and meaningful data consistent with the organization's incident response policy, plans, and procedures. **Met**	**Defined**
4.2.1.10	The organization has defined how it will meet the defined TIC security controls and ensure that all agency traffic, including mobile and cloud, are routed through defined access points, as appropriate. However, the organization has not ensured that the TIC 2.0 provider and agency managed capabilities are consistently implemented. **Met**	**Defined**
4.2.1.11	The organization has defined how it plans to utilize DHS' Einstein program for intrusion detection/prevention capabilities for traffic entering and leaving its networks. **Met**	**Defined**
4.2.1.12	The organization has defined how it plans to utilize technology to develop and maintain a baseline of network operations and expected data flows for users and systems. However, the organization has not established, and does not consistently maintain, a comprehensive baseline of network operations and expected data flows for users and systems. **Met**	**Defined**

Level 3

Definition

Section 4: Respond

4.3.1 In addition to the formalization and definition of its incident response program (Level 2), the organization consistently implements its incident response program across the agency, in accordance with FISMA (including guidance from NIST SP 800-83, NIST SP 800-61 Rev. 2, NIST SP 800-53, OMB M-16-03, OMB M-16-04, and US-CERT Federal Incident Notification Guidelines). However, data supporting metrics on the effectiveness of the incident response program across the organization are not verified, analyzed, and correlated.

People

4.3.1.1 Incident response team structures/models, stakeholders, and their roles, responsibilities, levels of authority, and dependencies have been fully defined, communicated, and consistently implemented across the organization (Level 2). Further, the organization has verified roles and responsibilities of incident response stakeholders as part of incident response testing. **Consistently Implemented**

Met

4.3.1.2 The organization has fully implemented its plans to close any gaps in the skills, knowledge, and resources needed to effectively implement its incident response program. Incident response teams are periodically trained to ensure that knowledge, skills, and abilities are maintained. **Consistently Implemented**

Met

4.3.1.3 The organization consistently utilizes its defined threat vector taxonomy and shares information with individuals with significant security responsibilities and other stakeholders in a timely fashion to support risk-based decision making. **Consistently Implemented**

Met

4.3.1.4 Incident response activities are integrated with organizational risk management, continuous monitoring, continuity of operations, and other mission/business areas, as appropriate. **Consistently Implemented**

Met

Processes

4.3.1.5 Incident response processes are consistently implemented across the organization for the following areas: incident response planning, incident response training and testing; incident detection and analysis; incident containment, eradication, and recovery; incident coordination, information sharing, and reporting using standard data elements and impact classifications within timeframes established by US-CERT. **Consistently Implemented**

Met

Section 4: Respond

4.3.1.6	The organization has ensured that processes to collaborate with DHS and other parties as appropriate, to provide on-site, technical assistance/surge resources/special capabilities for quickly responding to incidents are implemented consistently across the organization. **Met**	**Consistently Implemented**
4.3.1.7	The organization is consistently capturing qualitative and quantitative performance metrics on the performance of its incident response program. However, the organization has not ensured that the data supporting the metrics was obtained accurately and in a reproducible format or that the data is analyzed and correlated in ways that are effective for risk management. **Met**	**Consistently Implemented**
4.3.1.8	The organization is consistently collecting and capturing lessons learned and incident data on the effectiveness of its incident response program and activities. However, lessons learned may not be shared across the organization in a timely manner and used to make timely improvements to the incident response program and security measures. **Met**	**Consistently Implemented**
4.3.1.9	The rigor, intensity, scope, and results of incident response activities (i.e. preparation, detection, analysis, containment, eradication, and recovery, reporting and post incident) are comparable and predictable across the organization. **Met**	**Consistently Implemented**
Technology		
4.3.1.10	The organization has consistently implemented its defined incident response technologies in the following areas: - 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. The organization ensures that security and event data are aggregated and correlated from all relevant sources and sensors - Malware detection, such as anti-virus and antispam software technologies - Information management, such as data loss prevention - File integrity and endpoint and server security tools In addition, the tools are interoperable to the extent practicable, cover all components of the organization's network, and have been configured to collect and retain relevant and meaningful data consistent with the organization's incident response policy, procedures, and plans. **Met**	**Consistently Implemented**

Section 4: Respond

4.3.1.11	The organization has consistently implemented defined TIC security controls and implemented actions to ensure that all agency traffic, including mobile and cloud, are routed through defined access points, as appropriate. **Met**	**Consistently Implemented**
4.3.1.12	The organization is utilizing DHS' Einstein program for intrusion detection/prevention capabilities for traffic entering and leaving their networks. **Met**	**Consistently Implemented**
4.3.1.13	The organization has fully implemented technologies to develop and maintain a baseline of network operations and expected data flows for users and systems. **Met**	**Consistently Implemented**

Level 4

Definition

4.4.1 In addition to being consistently implemented (Level 3), incident response activities are repeatable and metrics are used to measure and manage the implementation of the incident response program, achieve situational awareness, and control ongoing risk. In addition, the incident response program adapts to new requirements and government-wide priorities.

People

4.4.1.1	Incident response stakeholders are consistently implementing, monitoring, and analyzing qualitative and quantitative performance measures across the organization and are collecting, analyzing, and reporting data on the effectiveness of the organization's incident response program. **Met**	**Managed and Measureable**
4.4.1.2	Skilled personnel have been hired and/or existing staff trained to develop the appropriate metrics to measure the success of the incident response program. **Met**	**Managed and Measureable**
4.4.1.3	Incident response stakeholders are assigned responsibilities for developing and monitoring incident response metrics, as well as updating and revising metrics as needed based on organization risk tolerance, the threat environment, business/mission requirements, and the results of the incident response program. **Met**	**Managed and Measureable**

Processes

Section 4: Respond

4.4.1.4	The organization has processes for consistently implementing, monitoring, and analyzing qualitative and quantitative performance measures across the organization and is collecting, analyzing, and reporting data on the effectiveness of its processes for performing incident response **Met**	**Managed and Measureable**
4.4.1.5	Data supporting incident response measures and metrics are obtained accurately, consistently, and in a reproducible format **Met**	**Managed and Measureable**
4.4.1.6	Incident response data, measures, and metrics are analyzed, collected, and presented using standard calculations, comparisons, and presentations **Met**	**Managed and Measureable**
4.4.1.7	Incident response metrics are reported to organizational officials charged with correlating and analyzing the metrics in ways that are relevant for risk management activities. **Met**	**Managed and Measureable**

Technology

4.4.1.8	The organization uses technologies for consistently implementing, 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. **Met**	**Managed and Measureable**
4.4.1.9	The organization's incident response performance measures include data on the implementation of its incident response program for all sections of the network. **Met**	**Managed and Measureable**

Level 5

Definition

4.5.1 In addition to being managed and measurable (Level 4), the organization's incident response program is institutionalized, repeatable, self-regenerating, and updated in a near real-time basis based on changes in business/mission requirements, and a changing threat and technology landscape.

People

Section 4: Respond

4.5.1.1	The organization's assigned personnel collectively possess a high skill level to perform and update incident response activities on a near real-time basis to make any changes needed to address incident response results based on organization risk tolerance, the threat environment, and business/mission requirements. **Met**	**Optimized**

Processes

4.5.1.2	The organization has institutionalized a process of continuous improvement incorporating advanced cybersecurity practices **Met**	**Optimized**
4.5.1.3	On a near real-time basis, the organization actively adapts its incident response program to a changing cybersecurity landscape and responds to evolving and sophisticated threats in a near real-time manner. **Met**	**Optimized**
4.5.1.4	The incident response program is fully integrated with organizational risk management, continuous monitoring, continuity of operations, and other mission/business areas, as appropriate **Met**	**Optimized**
4.5.1.5	The incident response program achieves cost-effective IT security objectives and goals and influences decision making that is based on cost, risk, and mission impact. **Met**	**Optimized**

Technology

4.5.1.6	The organization has institutionalized the implementation of advanced incident response technologies in near real-time **Met**	**Optimized**
4.5.1.7	The organization has institutionalized the use of advanced technologies for analysis of trends and performance against benchmarks to continuously improve its incident response program **Met**	**Optimized**
4.5.1.8	The organization uses simulation based technologies to continuously determine the impact of potential security incidents to its IT assets and adjusts incident response processes and security measures accordingly. **Met**	**Optimized**

Level	Score	Possible Score
LEVEL 5: Optimized	20	20

Section 5: Recover

Contingency Planning (Recover)

5.1	Has the organization established an enterprise-wide business continuity/disaster recovery program, including policies and procedures consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? **Met**	**Defined**
5.1.1	Develops and facilitates recovery testing, training, and exercise (TT&E) programs. (FCD1, NIST SP 800-34, NIST SP 800-53) **Met**	**Consistently Implemented**
5.1.2	Incorporates the system's Business Impact Analysis and Business Process Analysis into analysis and strategy toward development of the organization's Continuity of Operations Plan, Business Continuity Plan (BCP), and Disaster Recovery Plan (DRP). (NIST SP 800-34) **Met**	**Consistently Implemented**
5.1.3	Develops and maintains documented recovery strategies, plans, and procedures at the division, component, and IT infrastructure levels. (NIST SP 800-34) **Met**	**Consistently Implemented**
5.1.4	BCP and DRP are in place and ready to be executed upon if necessary. (FCD1, NIST SP 800-34, 2016 CIO FISMA Metrics 5.3, PMC) **Met**	**Consistently Implemented**
5.1.5	Tests BCP and DRP for effectiveness and updates plans as necessary. (2016 CIO FISMA Metrics, 5.4) **Met**	**Managed and Measureable**
5.1.6	Tests system-specific contingency plans, in accordance with organizationally defined timeframes, to determine the effectiveness of the plans as well as readiness to execute the plans if necessary. (NIST SP 800-53: CP-4) **Met**	**Consistently Implemented**
5.1.7	Develops after-action reports that address issues identified during contingency/disaster recovery exercises in order to improve contingency/disaster recovery processes. (FCD1, NIST SP 800-34) **Met**	**Managed and Measureable**

Section 5: Recover

5.1.8	Determines alternate processing and storage sites based upon risk assessments which ensure the potential disruption of the organization's ability to initiate and sustain operations is minimized, and are not subject to the same physical and/or cybersecurity risks as the primary sites. (FCD1, NIST SP 800-34, NIST SP 800-53: CP-6, CP-7) **Met**	**Consistently Implemented**
5.1.9	Conducts backups of information at the user- and system-levels and protects the confidentiality, integrity, and availability of backup information at storage sites. (FCD1, NIST SP 800-34, NIST SP 800-53: CP-9, NIST CF, PR.IP-4, NARA guidance on information systems security records) **Met**	**Managed and Measureable**
5.1.10	Contingency planning that considers supply chain threats. **Met**	**Defined**
5.1.11	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. Based on all testing performed is the Contingency Planning Program effective? **Effective**	

Level	Score	Possible Score
LEVEL 5: Optimized	20	20

APPENDIX A: Maturity Model Scoring

Maturity Levels by Section

Section	Level	Score	Possible Score
Section 1: Identify	LEVEL 3: Consistently Implemented	13	20
Section 2: Protect	LEVEL 3: Consistently Implemented	13	20
Section 3: Detect	LEVEL 4: Managed and Measureable	18	20
Section 4: Respond	LEVEL 5: Optimized	20	20
Section 5: Recover	LEVEL 5: Optimized	20	20
TOTAL		84	100
EFFECTIVE			

Section 1: Identify

Model Indicator	Met	Not Met	Total	%	Points Assigned	Possible Points
Ad-Hoc	0	0	0	100%	3	3
Defined	4	0	4	100%	4	4
Consistently Implemented	10	1	11	91%	6	6
Managed and Measureable	6	0	6	100%	0	5
Optimized	0	0	0	100%	0	2
NOT EFFECTIVE						

Section 2: Protect

Model Indicator	Met	Not Met	Total	%	Points Assigned	Possible Points
Ad-Hoc	0	0	0	100%	3	3
Defined	5	0	5	100%	4	4
Consistently Implemented	17	1	18	94%	6	6
Managed and Measureable	7	1	8	88%	0	5
Optimized	0	0	0	100%	0	2
NOT EFFECTIVE						

Section 3: Detect

Model Indicator	Met	Not Met	Total	%	Points Assigned	Possible Points
Ad-Hoc	10	0	10	100%	3	3
Defined	10	0	10	100%	4	4
Consistently Implemented	10	0	10	100%	6	6
Managed and Measureable	12	0	12	100%	5	5
Optimized	6	1	7	86%	0	2
EFFECTIVE						

Section 4: Respond

Model Indicator	Met	Not Met	Total	%	Points Assigned	Possible Points
Ad-Hoc	12	0	12	100%	3	3
Defined	12	0	12	100%	4	4
Consistently Implemented	13	0	13	100%	6	6
Managed and Measureable	9	0	9	100%	5	5
Optimized	8	0	8	100%	2	2
EFFECTIVE						

Section 5: Recover

Model Indicator	Met	Not Met	Total	%	Points Assigned	Possible Points
Ad-Hoc	0	0	0	100%	3	3
Defined	2	0	2	100%	4	4
Consistently Implemented	6	0	6	100%	6	6
Managed and Measureable	3	0	3	100%	5	5
Optimized	0	0	0	100%	2	2
EFFECTIVE						

Appendix 4
Report Distribution

Federal Labor Relations Authority

Ernest DuBester, Member
Patrick Pizzella, Member
Sarah Whittle Spooner, Executive Director
Michael Jeffries, Chief Information Officer
Fred Jacob, Solictor

CONTACTING THE OFFICE OF INSPECTOR GENERAL

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

HOTLINE (800)331-3572

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

EMAIL: OIGMAIL@FLRA.GOV
CALL: (202)218-7970 FAX: (202)343-1072
WRITE TO: 1400 K Street, N.W. Suite 250, Washington, D.C. 20424

The complainant may remain confidential; allow their name to be used; or anonymous. If the complainant chooses to remain anonymous, FLRA OIG cannot obtain additional information on the allegation, and also cannot inform the complainant as to what action FLRA OIG has taken on the complaint. Confidential status allows further communication between FLRA OIG and the complainant after the original complaint is received. The identity of complainants is protected under the provisions of the Whistleblower Protection Act of 1989 and the Inspector General Act of 1978. To learn more about the FLRA OIG, visit our Website at http://www.flra.gov/oig

Office of Inspector General

FISMA Evaluation