Inspector General

Section Report

2018

Annual FISMA Report

Equal Employment Opportunity Commission

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: CA-3, PM-5, and CM-8; OMB M-04-25; NIST 800-161; NIST Cybersecurity Framework (CSF): ID.AM-1 – 4; FY 2018 CIO FISMA Metrics: 1.1, 1.4, and 1.5)?

Managed and Measurable (Level 4)

Comments: The next level is not met because EEOC does not have an automated process to capture inventory data for all hardware and software components.

2 To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets connected to the organization's network with the detailed information necessary for tracking and reporting (NIST SP 800-53: CA-7 and CM-8; NIST SP 800-137; Federal Enterprise Architecture (FEA) Framework, v2; FY 2018 CIO FISMA Metrics: 1.2)?

Managed and Measurable (Level 4)

Comments: The next level is not met because EEOC does not employ automation to track the life cycle of all hardware components.

3 To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of the software and associated licenses used within the organization with the detailed information necessary for tracking and reporting (NIST SP 800-53: CA-7, CM-8, and CM-10; NIST SP 800-137; FEA Framework, v2)?

Managed and Measurable (Level 4)

Comments: The next level is not met because EEOC does not employ automation to track the life cycle of all software components.

4 To what extent has the organization categorized and communicated the importance/priority of information systems in enabling its missions and business functions (NIST SP 800-53: RA-2, PM-7, and PM-11; NIST SP 800-60; CSF: ID.BE-3; FIPS 199; FY 2018 CIO FISMA Metrics: 1.1)?

Consistently Implemented (Level 3)

Comments: Met

5 To what extent has the organization established, communicated, and implemented its risk management policies, procedures, and strategy that 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: 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; FY 2018 CIO FISMA Metrics: 1.6)?

Managed and Measurable (Level 4)

Comments: The next level is not met because EEOC’s risk management program is not embedded into daily decision making across the organization and does not provide for continuous risk identification.

Function 1: Identify - Risk Management

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 (NIST SP 800-39; FEA Framework; NIST SP 800-53: PL-8, SA-3, SA-8, SA-9, SA-12, and PM-9; NIST SP 800-161; DHS Binding Operational Directive 17-01)?

Defined (Level 2)

Comments: The next level is not met because EEOC does not consistently implement its security architecture across the enterprise, business process, and system levels.

7 To what degree have roles and responsibilities of stakeholders involved in risk management, including the risk executive function/Chief Risk Officer/Senior Accountable Official for Risk Management, Chief Information Officer, Chief Information Security Officer, and other internal and external stakeholders and mission specific resources been defined and communicated across the organization (NIST SP 800-39: Section 2.3.1 and 2.3.2; NIST SP 800-53: RA-1; CSF: ID.RM-1 – ID.GV-2; OMB A-123; CFO Council ERM Playbook)?

Managed and Measurable (Level 4)

Comments: The next level is not met because EEOC's risk management program does not address the full spectrum of an agency's risk portfolio across all organizational aspects.

8 To what extent has the organization ensured that plans of action and milestones (POA&Ms) are utilized for effectively mitigating security weaknesses (NIST SP 800-53: CA-5; OMB M-04-25)?

Managed and Measurable (Level 4)

Comments: The next level is not met because EEOC does not employ automation to correlate security weaknesses amongst information systems and identify enterprise-wide trends and solutions on a near real- time basis.

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 800-37; NIST SP 800-39; NIST SP 800-53: PL-2 and RA-1; NIST SP 800-30; CSF:ID.RA-1 – 6)?

Managed and Measurable (Level 4)

Comments: Met

Function 1: Identify - Risk Management

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))?

Consistently Implemented (Level 3)

Comments: The next level is not met because EEOC does not employ robust diagnostic and reporting frameworks, including dashboards that facilitate a portfolio view of interrelated risks across the organization.

11 To what extent does the organization ensure that specific contracting language (such as appropriate information security and privacy requirements and material disclosures, FAR clauses, and clauses on protection, detection, and reporting of information) and SLAs are included in appropriate contracts to mitigate and monitor the risks related to contractor systems and services (FAR Case 2007-004; Common Security Configurations; FAR Sections: 24.104, 39.101, 39.105, 39.106, and 52.239-1; President's Management Council; NIST SP 800-53: SA-4; FedRAMP standard contract clauses; Cloud Computing Contract Best Practices; FY 2018 CIO FISMA Metrics: 1.5; Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure)?

Managed and Measurable (Level 4)

Comments: Met

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)?

Defined (Level 2)

Comments: The next level is not met because EEOC has not implemented 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)

Comments: N/A

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?

N/A

Calculated Maturity Level - Managed and Measurable (Level 4)

Function 2A: Protect - Configuration Management

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

Consistently Implemented (Level 3)

Comments: MET

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: CM-9)?

Managed and Measurable (Level 4)

Comments: The next level is not met because EEOC does not have an automated process to change cybersecurity landscape on a near real-time basis.

16 To what degree have information system configuration management policies and procedures been defined and implemented across the organization? (Note: the maturity level should take into consideration the maturity of questions 17, 18, 19, and 21) (NIST SP 800-53: CM-1; NIST SP 800-128: 2.2.1)?

Managed and Measurable (Level 4)

Comments: The next level is not met because EEOC does not actively adapt its configuration management plan and related processes and activities to a changing cybersecurity landscape to respond to evolving and sophisticated threats on a real-time basis.

17 To what extent does the organization utilize baseline configurations for its information systems and maintain inventories of related components at a level of granularity necessary for tracking and reporting (NIST SP 800-53: CM-2 and CM-8; FY 2018 CIO FISMA Metrics: 1.1 and 2.2; CSF: ID.DE.CM-7)?

Consistently Implemented (Level 3)

Comments: The next level is not met because EEOC has not fully employ automated mechanisms to detect unauthorized hardware on its network.

18 To what extent does the organization utilize configuration settings/common secure configurations for its information systems? (NIST SP 800-53: CM-6, CM-7, and SI-2; FY 2018 CIO FISMA Metrics: 1.1 and 2.2; SANS/CIS Top 20 Security Controls 3.7)?

Optimized (Level 5)

Comments: MET

Function 2A: Protect - Configuration Management

19 To what extent does the organization utilize flaw remediation processes, including patch management, to manage software vulnerabilities (NIST SP 800-53: CM-3 and SI-2; NIST SP 800-40, Rev. 3; OMB M-16-04; SANS/CIS Top 20, Control 4.5; FY 2018 CIO FISMA Metrics: 2.13; and DHS Binding Operational Directive 15-01)?

Managed and Measurable (Level 4)

Comments: The next level is not met because EEOC does not utilize automated patch management and software update tools for all applications and network devices.

20 To what extent has the organization adopted the Trusted Internet Connection (TIC) program to assist in protecting its network (OMB M-08-05)?

Ad Hoc (Level 1)

Comments: The next level is not met because EEOC does not participate in the DHS Trusted Internet Connections (TIC) Initiative.

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: CM-2 and CM-3)?

Managed and Measurable (Level 4)

Comments: MET

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?

N/A

Calculated Maturity Level - Managed and Measurable (Level 4)

Function 2B: Protect - Identity and Access Management

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

Consistently Implemented (Level 3)

Comments: MET

Function 2B: Protect - Identity and Access Management

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

Defined (Level 2)

Comments: The next level is not met because EEOC has not consistently implemented its ICAM strategy to include stronger authentication (e.g. two-factors authentication).

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: AC-1 and IA-1; Cybersecurity Strategy and Implementation Plan (CSIP); SANS/CIS Top 20: 14.1; FY 2018 CIO FISMA Metrics: 2.3).

Managed and Measurable (Level 4)

Comments: The next level is not met because EEOC automated mechanism does not identify suspicious behavior and potential violations of its ICAM policies and procedures on a near-real time basis.

26 To what extent has the organization developed and implemented processes for assigning personnel risk designations and performing appropriate screening prior to granting access to its systems (NIST SP 800-53: PS-2 and PS-3; National Insider Threat Policy; FY 2018 CIO FISMA Metrics: 2.16)?

Managed and Measurable (Level 4)

Comments: The next level is not met because EEOC does not evaluate personnel security information from various sources, and integrate this information with anomalous user behavior data and inside threat on a real-time basis.

27 To what extent does the organization ensure that access agreements, including nondisclosure agreements, acceptable use agreements, and rules of behavior, as appropriate, for individuals (both privileged and non-privileged users) that access its systems are completed and maintained (NIST SP 800-53: AC-8, PL-4, and PS-6)?

Managed and Measurable (Level 4)

Comments: The next level is not met because EEOC does not ensure that access agreements for privileged and non-privileged users are updated on a real-time basis.

28 To what extent has the organization implemented strong authentication mechanisms (two-factor PIV credential or other NIST 800-63 r3 Identity Assurance Level (IAL)3/ Authenticator Assurance Level (AAL) 3/ Federated Assurance Level (FAL) 3 credential) for non-privileged users to access the organization's facilities, networks, and systems, including for remote access (CSIP; HSPD-12; NIST SP 800-53: AC-17; NIST SP 800-128; FIPS 201-2; NIST SP 800-63; FY 2018 CIO FISMA Metrics: 2.4; and Cybersecurity Sprint)?

Defined (Level 2)

Comments: The next level is not met because EEOC has not implemented strong authentication mechanisms (PIV) for non- privileged users of the organization’s facilities and networks, including for remote access, in accordance with Federal targets.

Function 2B: Protect - Identity and Access Management

29 To what extent has the organization implemented strong authentication mechanisms (two-factor PIV credential or other NIST 800-63 r3 IAL 3/ AAL 3/ FAL 3 credential) for privileged users to access the organization's facilities, networks, and systems, including for remote access (CSIP; HSPD-12; NIST SP 800-53: AC-17; NIST SP 800-128; FIPS 201-2; NIST SP 800-63; FY 2018 CIO FISMA Metrics: 2.5; and Cybersecurity Sprint)?

Defined (Level 2)

Comments: The next level is not met because EEOC has not implemented strong authentication mechanisms (PIV) for privileged users of the organization’s facilities and networks, including for remote access, in accordance with Federal targets.

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 2018 CIO FISMA Metrics: 2.4 and 2.5; NIST SP 800-53: AC-1, AC-2 (2), and AC-17; CSIP)?

Managed and Measurable (Level 4)

Comments: MET

31 To what extent does the organization ensure that appropriate configuration/connection requirements are maintained for remote access connections? This includes the use of appropriate cryptographic modules, system time-outs, and the monitoring and control of remote access sessions (NIST SP 800-53: AC-17 and SI-4; and FY 2018 CIO FISMA Metrics: 2.10)?

Consistently Implemented (Level 3)

Comments: The next level is not met because EEOC has not configured it information systems to restrict individual’s ability to transfer data accessed remotely to non-authorized devices.

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?

N/A

Calculated Maturity Level - Managed and Measurable (Level 4)

Function 2C: Protect - Data Protection and Privacy

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; OMB M-18-02; OMB A-130, Appendix I; NIST SP 800-53: AR-4 and Appendix J)?

Consistently Implemented (Level 3)

Comments: The next level is not met because EEOC does not monitor and analyses quantitative and qualitative performance measures on the effectiveness of its privacy activities and uses that information to make appropriate adjustments as needed.

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; Appendix J, SC-8, SC-28, MP-3, and MP-6; FY 2018 CIO FISMA Metrics: 2.9 and 2.10)?

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

Defined (Level 2)

Comments: The next level is not met because EEOC has not employed mechanism for the prevention and detection of untrusted removable media.

35 To what extent has the organization implemented security controls to prevent data exfiltration and enhance network defenses? (NIST SP 800-53: SI-3, SI-7(8), SI-4(4) and (18), SC-7(10), and SC-18; FY 2018 CIO FISMA Metrics: 3.8 – 3.12)?

Consistently Implemented (Level 3)

Comments: The next level is not met because EEOC does not measure the effectiveness of its data exfiltration and enhanced network defenses by conducting exfiltration exercises.

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: Appendix J, SE-2; FY 2018 SAOP FISMA metrics; OMB M-17-12; and OMB M-17-25)?

Consistently Implemented (Level 3)

Comments: The next level is not met because EEOC does not monitor and analyze its qualitative and quantitative performance measures on the effectiveness of its Data Breach Response Plan, as appropriate.

Function 2C: Protect - Data Protection and Privacy

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: 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)?

Managed and Measurable (Level 4)

Comments: The next level is not met because EEOC has not institutionalized a process of continuous improvement incorporating advanced privacy training practices and technologies.

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?

N/A

Calculated Maturity Level - Consistently Implemented (Level 3)

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: AT-1; and NIST SP 800-50).

Consistently Implemented (Level 3)

Comments: MET

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: 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)?

Ad Hoc (Level 1)

Comments: The next level is not met because EEOC has not defined a process for conducting assessment of the knowledge, skills, and abilities of its workforce.

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: AT-1; NIST SP 800-50: Section 3).

Consistently Implemented (Level 3)

Comments: The next level is not met because EEOC does not monitor and analyze qualitative and quantitative performance measures on the effectiveness of its security awareness and training strategies and plans.

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: AT-1 through AT-4; and NIST SP 800-50).

Consistently Implemented (Level 3)

Comments: The next level is not met because EEOC does not monitor and analyze qualitative and quantitative performance measures on the effectiveness of its security awareness and training policies and procedures.

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: AT-2; FY 2018 CIO FISMA Metrics: 2.15; NIST SP 800-50: 6.2; SANS Top 20: 17.4).

Managed and Measurable (Level 4)

Comments: The next level is not met because EEOC has not institutionalized a process of continuous improvement incorporating advanced security awareness practices and technologies.

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: AT-3 and AT-4; FY 2018 CIO FISMA Metrics: 2.15)?

Consistently Implemented (Level 3)

Comments: The next level is not met because EEOC does not obtain feedback on its security training content and makes updates to its program, as appropriate.

Function 2D: Protect - Security Training

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

Consistently Implemented (Level 3)

Comments: N/A

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?

N/A

Calculated Maturity Level - Consistently Implemented (Level 3)

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 organization-wide approach to ISCM (NIST SP 800-137: Sections 3.1 and 3.6)?

Managed and Measurable (Level 4)

Comments: The next level is not met because EEOC’s ISCM strategy is not fully integrated with its risk management, configuration management, incident response, and business continuity functions.

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: CA-7) (Note: The overall maturity level should take into consideration the maturity of question 49)?

Managed and Measurable (Level 4)

Comments: The next level is not met because EEOC’s ISCM policies and procedures are not fully integrated with its risk management, configuration management, incident response, and business continuity functions.

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: CA-1; NIST SP 800-137; and FY 2018 CIO FISMA Metrics)?

Managed and Measurable (Level 4)

Comments: MET

Function 3: Detect - ISCM

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: CA-2, CA-6, and CA-7; NIST Supplemental Guidance on Ongoing Authorization; OMB M-14-03)?

Managed and Measurable (Level 4)

Comments: The next level is not met because the EEOC ISCM program IT security objectives and goals are not supported by cost-effective decision making that is based on cost, risk, and mission impact.

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 next level is not met because EEOC is unable 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 - ISCM function.

Managed and Measurable (Level 4)

Comments: N/A

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?

N/A

Calculated Maturity Level - Managed and Measurable (Level 4)

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: 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: 4.1, 4.3, 4.6, and 5.3; Presidential Policy Direction (PPD) 41)? (Note: The overall maturity level should take into consideration the maturity of questions 53 - 58)?

Consistently Implemented (Level 3)

Comments: The next level is not met because EEOC does not monitor and analyze qualitative and quantitative performance measures on the effectiveness of its incident response policies, procedures, plans, and strategies, as appropriate.

Function 4: Respond - Incident Response

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: IR-7; NIST SP 800-83; NIST SP 800-61 Rev. 2; OMB M-18-02; OMB M-16-04; FY 2018 CIO FISMA Metrics: Section 4; and US-CERT Federal Incident Notification Guidelines)?

Managed and Measurable (Level 4)

Comments: MET

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; and US-CERT Incident Response Guidelines)?

Consistently Implemented (Level 3)

Comments: The next level is not met because EEOC does not utilize profiling techniques to measure the characteristics of expected activities on its networks and systems to detect security incidents such as file integrity checking software for critical files.

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

Managed and Measurable (Level 4)

Comments: The next level is not met because EEOC does not utilize dynamic reconfiguration to stop attacks, misdirect attackers, and to isolate components of 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: IR-6; US-CERT Incident Notification Guidelines; PPD-41; DHS Cyber Incident Reporting Unified Message)?

Managed and Measurable (Level 4)

Comments: MET

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 (FY 2018 CIO FISMA Metrics: 4.4; NIST SP 800-86; NIST SP 800-53: IR-4; OMB M-18-02; PPD-41).

Managed and Measurable (Level 4)

Comments: MET

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 next level is not met because EEOC does not uses technologies for monitoring and analyzing qualitative and quantitative performance across the organization and 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.

Managed and Measurable (Level 4)

Comments: N/A

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?

N/A

Calculated Maturity Level - Managed and Measurable (Level 4)

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

Consistently Implemented (Level 3)

Comments: MET

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; FY 2018 CIO FISMA Metrics: 5.1, 5.2, and 5.5).

Managed and Measurable (Level 4)

Comments: The next level is not met because EEOC's information system contingency planning program is not fully integrated with the enterprise risk management program.

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: CP-2; NIST SP 800-34, Rev. 1, 3.2; FIPS 199; FCD-1; OMB M-17-09; FY 2018 CIO FISMA Metrics: 5.6)?

Consistently Implemented (Level 3)

Comments: MET

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: CP-2; NIST SP 800-34; FY 2018 CIO FISMA Metrics: 5.1, 5.2, and 5.5)?

Consistently Implemented (Level 3)

Comments: The next level is not met because EEOC is unable to integrate metrics on the effectiveness of its information system contingency plans with information on the effectiveness of related plans.

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: CP-3 and CP-4; FY 2018 CIO FISMA Metrics: 5.1, 5.2, and 5.5)?

Consistently Implemented (Level 3)

Comments: The next level is not met because EEOC does not employ automated mechanisms to more thoroughly and effectively test system contingency plans.

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: 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 2018 CIO FISMA Metrics: 5.4; and NARA guidance on information systems security records)?

Consistently Implemented (Level 3)

Comments: MET

Function 5: Recover - Contingency Planning

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: CP-2 and IR-4)?

Consistently Implemented (Level 3)

Comments: MET

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

Consistently Implemented (Level 3)

Comments: N/A

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?

N/A

Calculated Maturity Level - Consistently Implemented (Level 3)

Function 0: Overall

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

Effective

Comments: N/A

Function 0: Overall

0.2 Please provide an overall assessment of the agency's information security program. The narrative should include a description of the assessment scope, a summary on why the information security program was deemed effective/ineffective and any recommendations on next steps. Please note that OMB will include this information in the publicly available Annual FISMA Report to Congress to provide additional context for the Inspector General's effectiveness rating of the agency's information security program. OMB may modify the response to conform with the grammatical and narrative structure of the Annual Report.

We utilized the Final FY 2018 Inspector General FISMA Metrics v1.0 maturity model to access the maturity of the EEOC's information system security program. The metrics include eight functional areas and related category. Ratings throughout the eight function areas were by a simple majority, where the most frequent level (i.e., the mode) across the questions served as the function area rating. For example, if there are seven questions in a function area, and the EEOC received defined ratings for three questions and managed and measurable ratings for four questions, then the function area rating is managed and measurable.

The overall assessment of the EEOC information system program is "Level 4: Managed and Measurable." EEOC information system program could be improve by developing qualitative and quantitative performance measures and metrics in the areas of Protect and Recover.

APPENDIX A: Maturity Model Scoring

Function 1: Identify - Risk Management

Function	Count
Ad-Hoc	0
Defined	2
Consistently Implemented	2
Managed and Measurable	8
Optimized	0
Function Rating: Managed and Measurable (Level 4)Effective	0

Function 2A: Protect - Configuration Management

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

Function 2B: Protect - Identity and Access Management

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

Function 2C: Protect - Data Protection and Privacy

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

Function 2D: Protect - Security Training

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

Function 3: Detect - ISCM

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

Function 4: Respond - Incident Response

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

Function 5: Recover - Contingency Planning

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

Maturity Levels by Function

Function	Calculated Maturity Level	Assessed Maturity Level	Explanation
Function 1: Identify - Risk Management	Managed and Measurable (Level 4)	Managed and Measurable (Level 4)	N/A
Function 2: Protect - Configuration Management / Identity & Access Management / Data Protection & Privacy / Security Training	Managed and Measurable (Level 4)	Consistently Implemented (Level 3)	N/A
Function 3: Detect - ISCM	Managed and Measurable (Level 4)	Managed and Measurable (Level 4)	N/A
Function 4: Respond - Incident Response	Managed and Measurable (Level 4)	Managed and Measurable (Level 4)	N/A
Function 5: Recover - Contingency Planning	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	N/A
Overall	Effective	Effective	