Independent Evaluation of the U.S. Equal Employment Opportunity Commission's Compliance with Provisions of the Federal Information Security Modernization Act of 2014 (FISMA)

For Fiscal Year 2017
2017-07-AOIG

Prepared by:

Brown & Company
Certified Public Accountants and Management Consultants, PLLC
1101 Mercantile Lane, Suite 122
Largo, Maryland 20774
(240) 770-4903

December 18, 2017

Independent Evaluation of the U.S. Equal Employment Opportunity Commission's Compliance with Provisions of the Federal Information Security Modernization Act of 2014 (FISMA)

Table of Contents

Independent Auditor's Report

Inspector General of the
U.S. Equal Employment Opportunity Commission:

This report presents the results of Brown & Company CPAs and Management Consultants, PLLC (Brown & Company) independent audit of the U.S. Equal Employment Opportunity Commission's (EEOC) Information Security Program and practices in accordance with the Federal Information Security Modernization Act of 2014 (FISMA). The EEOC Office of Inspector General (OIG) contracted with Brown & Company to conduct this independent audit of EEOC's Information Security Program and practices as a performance audit under generally accepted government auditing standards (GAGAS).

FISMA requires EEOC to develop, document, and implement an agency-wide Information Security Program to protect its information and information systems, including those provided or managed by another agency, contractor, or other source. Additionally, FISMA requires EEOC to undergo an annual independent evaluation of its information security program and practices, as well as an evaluation of the effectiveness of information security programs and controls.

FISMA re-emphasizes the Chief Information Officer's (CIO) strategic, agency-wide security responsibility. At EEOC, security responsibility is assigned to the agency's Office of Information Technology (OIT). FISMA also clearly places responsibility on each agency program office to develop, implement, and maintain a security program that assesses risk and provides adequate security for the operations and assets of programs and systems under its control.

The objectives of this performance audit were to evaluate the effectiveness of the EEOC's Information Security Program and practices and respond to the Department of Homeland Security's (DHS) *FY 2017 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics V 1.0*, dated April 17, 2017. The scope of the audit includes assessing the effectiveness and efficiency of EEOC's information security programs and practices, and whether they meet the requirements of FISMA for the fiscal year ending September 30, 2017.

Brown & Company's methodology for the FY 2017 FISMA audit included testing the EEOC's General Support System (GSS) and other systems for compliance with selected controls covered by the National Institute of Standards and Technology's (NIST) Special Publication (SP) 800-53, Revision (Rev.) 4, *Security and Privacy Controls for Federal Information Systems and Organizations.*

1101 MERCANTILE LANE, SUITE 122 • LARGO, MD 20774
PHONE: (240) 770-4900 • FAX: (301) 773-2090 • mail@brownco-cpas.com • www.brownco-cpas.com

We considered the internal control structure for various EEOC systems in planning our audit procedures. These procedures were mainly substantive in nature, although we did gain an understanding of management procedures and controls to the extent necessary to achieve our audit objectives. Accordingly, we obtained an understanding of the internal controls for these various systems through interviews and observations, as well as inspection of various documents, including information technology and other related organizational policies and procedures.

We conducted this performance audit in accordance with GAGAS. Those standards require that we plan and perform the audit to obtain sufficient and appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions according to our audit objectives.

We found that EEOC generally had sound information security controls for its Information Security Program and has implemented security controls in all seven DHS Inspector General (IG) FISMA Reporting Metrics. Based on our audit work, we concluded that the EEOC's Information Security Program is generally compliant with the FISMA legislation and applicable Office of Management and Budget (OMB) guidance and the security controls tested demonstrated operating effectiveness.

Our report identifies the following four control weaknesses where the EEOC's Information Security Program can better protect the confidentiality, integrity, and availability of its information and information systems:

1. The EEOC has not implemented automated solution that provides a centralized, enterprise-wide view of risk across the agency.
2. The EEOC has not developed a Trusted Internet Connection (TIC) program that meets OMB requirements to improve the agency's security posture.
3. The EEOC has not conducted an e-authentication risk assessment for its digital systems and has did not fully implement multifactor authentication for logical and remote access for privileged and non-privileged users.
4. Separation of duties between the Chief Information Security Officer (CISO) and Deputy Chief Information Officer (DCIO) positions.

Addressing these four control weaknesses strengthens the EEOC's Information Security Program, and contributes to ongoing efforts to maintain reasonable assurance of adequate security over information resources.

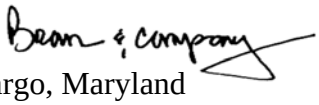
This report makes four recommendations to assist EEOC in strengthening its Information Security Program.

This performance audit did not constitute an audit of financial statements in accordance with GAGAS. Brown & Company was not engaged to, and did not, render an opinion on EEOC's internal controls over financial reporting or financial management systems. Furthermore, the projection of any conclusions based on our findings to future periods is subject to the risk that

controls may become inadequate due to changes in conditions or the deterioration of compliance with controls.

This report is intended solely for the information and use of the management of EEOC, OIG, and the U.S. Congress, and is not intended to be, and should not be, used by anyone other than these specified parties.

In closing, we appreciate the courtesies extended to Brown & Company Audit Team by EEOC and EEOC OIG during this engagement.



Largo, Maryland
December 18, 2017

1. Executive Summary

For Fiscal Year (FY) 2017, the U.S. Equal Employment Opportunity Commission (EEOC), Office of Inspector General (OIG) contracted with Brown & Company CPAs and Management Consultants, PLLC (Brown & Company) to conduct an independent evaluation of EEOC's compliance with the provisions of the Federal Information Security Modernization Act of 2014 (FISMA). FISMA requires agencies to develop, document, and implement an agency-wide information security program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

The EEOC Office of Information Technology (OIT) is responsible for planning, developing, implementing and maintaining EEOC's Information Technology (IT) program, policies, standards and procedures. OIT promotes the application and use of information technologies and administers policies and procedures within EEOC to ensure compliance with related federal laws and regulations, to include information security. OIT is responsible for designing the enterprise information architecture; determining the requirements of EEOC's information systems; and developing the integrated systems for nationwide use. The OIT consists of three components: Immediate Office of the Chief Information Officer (OCIO); Customer Services Management Division, Infrastructure Management and Operations Division; and Enterprise Applications Innovation Division.

Overall Assessment of EEOC Information Security Program

Based on the results of our evaluation, Brown & Company concluded that EEOC's Information Security Program is generally compliant with the FISMA legislation and applicable Office of Management and Budget (OMB) guidance. EEOC continues to make positive strides in addressing information security weaknesses. We found that EEOC's information security programs are effective and provide reasonable assurance of adequate security.

In conducting our audit work, we identified the following four control weaknesses related to EEOC security practices that can be improved:

1. The EEOC has not implemented automated solution that provides a centralized, enterprise-wide view of risk across the agency.
2. The EEOC has not developed a Trusted Internet Connection (TIC) program that meets OMB requirements to improve the agency's security posture.
3. The EEOC has not conducted an e-authentication risk assessment for its digital systems and has did not fully implement multifactor authentication for logical and remote access for privileged and non-privileged users.
4. Separation of duties between the Chief Information Security Officer (CISO) and Deputy Chief Information Officer (DCIO) positions.

2. Background

The EEOC Overview

The U.S. Equal Employment Opportunity Commission (EEOC) is a bipartisan Commission comprised of five presidentially appointed members, including the Chair, Vice Chair, and three Commissioners. The Chair is responsible for the administration and implementation of policy for and the financial management and organizational development of the Commission. The Vice Chair and the Commissioners participate equally in the development and approval of Commission policies, issue charges of discrimination where appropriate, and authorize the filing of suits. In addition to the Commissioners, the President appoints a General Counsel to support the Commission and provide direction, coordination, and supervision to the EEOC's litigation program.

The EEOC is responsible for enforcing federal laws that make it illegal to discriminate against a job applicant or an employee because of the person's race, color, religion, sex (including pregnancy, gender identity, and sexual orientation), national origin, age (40 or older), disability or genetic information. It is also illegal to discriminate against a person because the person complained about discrimination, filed a charge of discrimination, or participated in an employment discrimination investigation or lawsuit. EEOC provides services at the headquarters offices in Washington, D.C. and through 53 field offices.

The Federal Information Security Modernization Act of 2014

On December 18, 2014, the President signed the Federal Information Security Modernization Act (FISMA) of 2014, a bill that reformed the FISMA of 2002. The law updates and modernizes FISMA to provide a leadership role for the Department of Homeland Security (DHS), and includes security incident reporting requirements, and other key changes. The amended FISMA places greater management and oversight attention on data breaches, evaluating the effectiveness of security controls and configurations, and security control monitoring processes and procedures. This update provides several modifications to FISMA that modernize federal security practices to current security concerns. Specifically, the bill:

- Reasserts the authority of the Director of the OMB with oversight, while authorizing the Secretary of DHS to administer the implementation of security policies and practices for federal information systems.
- Gives the delegation of OMB's authorities to the Director of National Intelligence (DNI) for systems operated by an element of the intelligence community.
- Requires agencies to notify Congress of major security incidents within 7 days.
- Places more responsibility on agencies looking at budgetary planning for security management, ensuring senior officials accomplish information security tasks, and that all personnel are responsible for complying with agency information security programs.
- Changes the reporting guidance to focus on threats, vulnerabilities, incidents, and the compliance status of systems at the time of major incidents, and data on incidents involving Personally Identifiable Information (PII).

- Calls for the revision of OMB Circular A-130 to eliminate inefficient or wasteful reporting.
- Provides for the use of automated tools in agencies' information security programs, including periodic risk assessments; testing of security procedures; and detecting, reporting, and responding to security incidents.

Furthermore, OIG must submit to OMB the "Inspector General FISMA Reporting Metrics" that depicts the effectiveness of the agency's information security program.

OMB is responsible for reporting to Congress a summary of the results of agency compliance with FISMA requirements. OMB's principle written statement of Government policy regarding information security, OMB Circular No. A-130, *Management of Federal Information Resources*, Appendix III, *Security of Federal Automated Information Resou*rces, dated November 28, 2000, establishes a minimum set of controls to be included in federal automated information security programs. In particular, OMB Circular A-130, Appendix III defines adequate security as security commensurate with the risk and magnitude of the harm resulting from loss, misuse, or unauthorized access to, or modification of, information. This includes ensuring that systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability through the use of cost-effective management, personnel, operational, and technical controls.

On July 27, 2016, OMB released a revised Circular A-130, *Managing Federal Information as a Strategic Resource*. This revised circular continues to establish minimum requirements for federal information security programs, and assigns responsibilities for the security of information and information systems to the agency's CIO and others. The revised Circular A-130 adopts the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) and the NIST Cybersecurity Framework, requiring agencies to perform ongoing re-authorizations of systems and replace the triennial reauthorization process to better protect agency information and information systems. In certain areas, the revised Circular A-130 expands upon a minimum set of security controls required in NIST Special Publication (SP) 800-53, Revision (Rev.) 4. Specifically, the revised Circular A-130 adds requirements for moderate and high-impact systems to have PII encrypted at rest and in transit and instructs federal agencies to periodically test response procedures and document lessons-learned to improve incident response.

3. Audit Objectives

The objective of this independent evaluation is to conduct a review of EEOC's information security program and practices as required by FISMA. The objective involved reviewing the effectiveness and efficiency of the agency's information security program.

4. Audit Scope

The scope of the independent evaluation is to determine the effectiveness and efficiency of EEOC's information security program and practices, and whether EEOC meets the requirements

of FISMA. In assessing EEOC's adherence with FISMA, the following **Exhibit 1** NIST cybersecurity framework function areas and domains[1] were reviewed:

Exhibit 1 – FY 2017 IG FISMA Reporting Metrics

NIST Cybersecurity Framework Functions	NIST Cybersecurity Framework Domains
Identify Function Area	Risk Management
Protect Function Area	Configuration Management
	Identify and Access Management
	Security Training
Detect Function Area	Information Security Continuous Monitoring (ISCM)
Respond Function Area	Incident Response
Recover Function Area	Contingency Planning

The period covered by this independent evaluation is October 1, 2016 to September 30, 2017. The work was performed in accordance with generally accepted government auditing standards (GAGAS).

The scope includes reviewing the effectiveness of EEOC's information security program and evaluating the following information systems:

- DataNet System (DNS)
- Document Management System (DMS)
- Integrated Mission System (IMS)
- Federal Personnel Payroll System (FPPS)
- DOI Interior Business Center, Oracle Federal Financials (OFF)
- EEO-1 Survey System.

5. Testing Methodology

Brown & Company's testing methodology included: interviews with EEOC management and staff review of legal and regulatory requirements, performance of audit procedures, and review of documentation relating to EEOC's information security program. We utilized the Final FY 2017 IG FISMA Metrics v1.0 maturity model[2] to assess the maturity of the organization's information system security program. See **Appendix A**: *FY 2017 Inspector General FISMA Metrics Results* for details.

6. Summary of Results

FISMA requires each federal agency to develop and implement an agency-wide Information Security Program to address security for the information and information systems that support the

[1] *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.0, National Institute of Standards and Technology, February 12, 2014, defines the NIST functions and categories.
[2] FY 2017 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics V 1, April 17, 2017.

operations and assets of the agency, including those provided or managed by another organization, contractor, or other source. In addition, FISMA requires each agency's IG to conduct an independent evaluation to determine the effectiveness of the information security program and practices of its respective agency.

On behalf of the EEOC OIG, Brown & Company has assessed the effectiveness of EEOC information system security controls and identified weaknesses. We found that the EEOC Information Security Program is generally in compliance with FISMA legislation and OMB guidance, and it provides reasonable assurance of adequate security.

The **Exhibit 2** summarizes the results on the effectiveness of EEOC's information security controls.

Exhibit 2 – EEOC Security Control Effectiveness

FISMA NIST Cybersecurity Framework Functions	**FISMA NIST Cybersecurity Framework Domains**	**FISMA Security Control Effectiveness**
Identify	Risk Management	EEOC demonstrated effectiveness
Protect	Configuration Management	EEOC demonstrated effectiveness
	Identify and Access Management	EEOC demonstrated effectiveness
	Security Training	EEOC demonstrated effectiveness
Detect	Information Security Continuous Monitoring (ISCM)	EEOC demonstrated effectiveness
Respond	Incident Response	EEOC demonstrated effectiveness
Recover	Contingency Planning	EEOC demonstrated effectiveness

We found that EEOC's information security programs have an overall maturity level of "Managed and Measurable" based on the FY 2017 DHS IG FISMA Metric functions against the criteria listed below. **Exhibit 3** provides our overall assessment of EEOC's maturity level by function area. **Exhibit 4** provides DHS maturity level criteria.

Exhibit 3 – EEOC Overall Maturity Level Assessment by Functions Area

FISMA NIST Cybersecurity Framework Functions Area (Domains)	**Overall Maturity Level**
Function 1: Identify (Risk Management)	Optimized (Level 5)
Function 2: Protect (Configuration Management)	Managed and Measurable (Level 4)
Function 2: Protect (Identity and Access Management)	Managed and Measurable (Level 4)
Function 2: Protect (Security Training)	Managed and Measurable (Level 4)
Function 3: Detect (Information Security Continuous Monitoring (ISCM))	Managed and Measurable (Level 4)
Function 4: Respond (Incident Response)	Consistently Implemented (Level 3)
Function 5: Recover (Contingency Planning)	Managed and Measurable (Level 4)

Exhibit 4 – DHS Maturity Level Criteria

Maturity Level Criteria	Maturity Level Description
Level 1: Ad hoc	Policies, procedures, and strategy are not formalized; activities are performed in an ad hoc, reactive manner.
Level 2: Defined	Policies, procedures, and strategy are formalized and documented, but not consistently implemented.
Level 3: Consistently Implemented	Policies, procedures, and strategy are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.
Level 4: Managed and Measurable	Quantitative and qualitative measures on the effectiveness of policies, procedures, and strategy are collected across the organization and used to assess and make necessary changes.
Level 5: Optimized	Policies, procedures, and strategy are fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business/mission needs.

In conducting our audit work, Brown & Company identified the following four control weaknesses related to EEOC information security program that can be improved:

1. The EEOC has not implemented automated solution that provides a centralized, enterprise-wide view of risk across the agency.
2. The EEOC has not developed a TIC program that meets OMB requirements to improve the agency's security posture.
3. The EEOC has not conducted an e-authentication risk assessment for its digital systems and has did not fully implement multifactor authentication for logical and remote access for privileged and non-privileged users.
4. Separation of duties between the CISO and DCIO positions.

7. Findings and Recommendations

The results of our independent evaluation identified areas in EEOC's information security program that need improvement. The four findings and four recommendations are discussed below.

Finding 1: The EEOC has not implemented automated solution that provides a centralized, enterprise-wide view of risk across the agency.

Condition

The EEOC OIT has not implemented an automated solution that provides a centralized, enterprise-wide view of risk across the agency. In 2017, the EEOC formally defined its Enterprise Risk Management (ERM) program. The EEOC has developed an ERM Policy Handbook that includes a comprehensive strategy for managing risk across the agency. The EEOC OIT's process for managing its risk portfolio includes preparing schedules that capture and manage risk profiles, risk rankings, risk registers and Plan of Action and Milestones (POAMs). The schedules are routed to the ERM committee stakeholders for review. The EEOC OIT plans to implement ServiceNow

Governance, Risk, and Compliance (GRC) application to provide a centralized, enterprise- wide view of risk across the agency. However, they have not developed a formal plan or set a timeframe for the implementation.

Criteria

NIST Special Publication 800-39, Managing Information Security Risk, Organization, Mission, and Information System View states:

> Where automated monitoring is feasible, it should be employed because it is generally faster, more efficient, and more cost-effective than manual monitoring. Automated monitoring is also less prone to human error.

Cause

EEOC OIT has not developed a formal plan to implement an automated solution that provides a centralized, enterprise-wide view of risk across the agency. As stated in the "ERM Policy Handbook", EEOC's risk assessment tools and techniques will evolve as the agency implements its revised ERM program.

Effect

The implementation of an automated centralized enterprise-wide tool can improve the efficiency of managing risk across the agency.

Recommendation 1

We recommend the EEOC OIT implement an automated solution to provide a centralized, enterprise-wide view of risk across the agency.

Management's Response

EEOC's management provided the following response to the finding and recommendation:

> *OIT concurs with the recommendation and previously met with the Office of Research, Information, and Planning to commit to implementing a SharePoint solution for this requirement during FY 2018.*

Auditor's Evaluation of Management's Response

EEOC's management concurred with the recommendations.

Management's full response is provided in **Appendix C.**

Finding 2: The EEOC has not developed a Trusted Internet Connection (TIC) program that meets OMB requirements to improve the agency's security posture.

Condition

The EEOC OIT has not developed a TIC program that meets OMB requirements to improve the agency's security posture. Also, EEOC has not adequately prepared and planned to meet the goals of the DHS TIC initiative. Specifically, EEOC OIT does not have plans for reducing and consolidating EEOC's external connections, routing the agency's traffic through defined access points, and meeting the critical TIC security controls.

The EEOC OIT participates in the DHS Continuous Diagnostics and Mitigation (CDM) program that provides network protection and vulnerability scanning. The program includes implementing DHS's EINSTEIN Accelerated (E3A) system with intrusion prevention capability to identify and block cyber-attacks for federal agencies. The EEOC OIT has implemented the aggregation and Domain Name Server (DNS) Sinkholing components of E3A. Going forward, the EEOC OIT plans to implement the email filtering component of E3A. However, the EEOC OIT has not developed a TIC program required by OMB.

Criteria

NIST Special Publication 800-53, Revision 4*, Security and Privacy Controls for Federal Information Systems and Organizations,* SC-7(3) "Boundary Protection | Access Points," states**:**

> Control:
>
> The organization limits the number of external network connections to the information system.
> Supplemental Guidance: Limiting the number of external network connections facilitates more comprehensive monitoring of inbound and outbound communications traffic. The Trusted Internet Connection (TIC) initiative is an example of limiting the number of external network connections.
>
> **OMB Requirements:**
>
> The OMB Memorandum M-08-05, *Implementation of Trusted Internet Connections* (TIC), dated November 20, 2007, announced the Trusted Internet Connections (TIC) initiative to optimize federal individual network services into a common solution for the federal government. This common solution facilitates the reduction of federal external connections, including federal Internet points of presence, to a target of fifty. Additionally, the role of the US-CERT will be enhanced to improve federal response capabilities.
>
> In accordance with OMB Memorandum M-08-16, *Guidance for Trusted Internet Connection Statement of Capability (SOC),* TIC Access Provider (TICAP) agency Chief Information Officers should determine the gap between their agency's current capabilities

and the 51 capabilities identified in the Statement of Capability document. Appendix B of the TIC Reference Architecture explains the 51 critical technical capabilities.

OMB Memorandum M-08-26, *Transition from FTS2001 to NETWORX,* states that to improve federal agency's security posture with TIC-compliant managed security services, agencies are encouraged to purchase the Managed Trusted Internet Protocol Services (MTIPS) CLIN through the Networx Contract.

OMB Memorandum M-08-27, *Guidance for Trusted Internet Connection (TIC) Compliance,* provide further guidance to agencies on the steps necessary to complete the TIC Cybersecurity Capability Validation (CCV).

OMB Memorandum M-09-32: *Update on the Trusted Internet Connections Initiative*, states: Federal policy requires all agencies to undertake immediate responsibility for executing essential agreements and updating Plans of Action and Milestones (POA&Ms) to facilitate not only TIC preparations, but also due diligence for integrating the National Cyber Protection System (NCPS, operationally referred to as Einstein) deployments and synchronizing with US-CERT.

Cause

The EEOC OIT has not developed and implemented a TIC program due to lack of funding. The EEOC OIT has taken part in the DHS CDM program that provides network protection and vulnerability scanning.

Effect

Reducing the number of access points across the agency reduces EEOC's exposure to threats as fewer access points are open for Internet intrusions.

Recommendation 2

We recommend the EEOC Office of Information Technology develop and implement a Trusted Internet Connection (TIC) program in accordance with Office of Management and Budget (OMB) requirements to assist in protecting the agency's network from cyber threats.

Management's Response

EEOC's management provided the following response to the finding and recommendation:

> *OIT agrees that EEOC has not acquired TIC Managed Trusted Internet Protocol Services (MTIPS), primarily due to funding constraints. EEOC is participating in the related DHS Einstein 3A (E3A) programs to enhance cybersecurity analysis, situational awareness, and security response. OIT has aggregated all Internet traffic to route through DHS E3A and deployed E3A DNS sink-holing. The third and final component of E3A, email filtering, will occur after DHS has successfully piloted these services with Office 365. EEOC will evaluate TIC MTIPS benefits over Einstein 3A and, potentially, procure these services in FY 2018.*

Auditor's Evaluation of Management's Response

EEOC's management partially concurred with the recommendations. We noted that EEOC will evaluate TIC MTIPS benefits over Einstein 3A and, potentially, procure these services in FY 2018.

Management's full response is provided in **Appendix C.**

Finding 3:	**The EEOC has not conducted an e-authentication risk assessment for its digital systems and has did not fully implement multifactor authentication for logical and remote access for privileged and non-privileged users.**

Condition

The EEOC OIT has not conducted an e-authentication risk assessment of its digital systems and has did not fully implement multifactor authentication for logical and remote access for privileged and non-privileged users. EEOC's new digital services include Online Charge Status System and Digital Charge System. The EEOC OIT has not conducted an e-authentication risk assessment to determine the appropriate level of assurance needed for its digital systems.

Also, the EEOC OIT has not fully implemented multifactor authentication for logical and remote access for privileged and non-privileged users for its information systems. The EEOC OIT has implemented Active Directory to support two-factor authentication for its information systems using PIV cards. The EEOC OIT plans to take a phased approach in implementing two-factor authentication. The first phase will include privilege users and a pilot remote logical access program. The second phase will include non-privileged users.

Criteria:

NIST Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations,* IA-2 "Identification and Authentication" (Organizational Users), states:

> Control: The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).
>
> Identification and Authentication/Acceptance of PIV Credentials
>
> The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials.
>
> Supplemental Guidance: "This control enhancement applies to organizations implementing logical access control systems (LACS) and physical access control systems (PACS). Personal Identity Verification (PIV) credentials are those credentials issued by federal agencies that conform to FIPS Publication 201 and supporting guidance documents. OMB Memorandum 11-11 requires federal agencies to continue implementing the requirements specified in HSPD-12 to enable agency-wide use of PIV credentials."

NIST Special Publication 800-63-3, Digital Identity Guidelines, states**:**

> Agencies use these guidelines as part of the risk assessment and implementation of their digital service(s). It provides an overview of general identity frameworks, using authenticators, credentials, and assertions together in a digital system, and a risk-based process of selecting assurance levels

NIST Special Publication 800-63-A, Digital Identity Guidelines, *Enrollment and Identity Proofing,* states:

> How applicants can prove their identities and become enrolled as valid subscribers within an identity system. It provides requirements by which applicants can both identity proof and enroll at one of three different levels of risk mitigation in both remote and physically-present scenarios.
>
> SP 800-63A sets requirements to achieve a given level of assurance (IAL). The three IALs reflect the options agencies may select from based on their risk profile and the potential harm caused by an attacker making a successful false claim of an identity.

NIST Special Publication 800-63-B, Authentication and Lifecycle Management, states:

> For services in which return visits are applicable, a successful authentication provides reasonable risk-based assurances that the subscriber accessing the service today is the same as that which accessed the service previously.

NIST Special Publication 800-63-C, Digital Identity Guidelines, *Federation and Assertions,* states:

> Provides requirements when using federated identity architectures and assertions to convey the results of authentication processes and relevant identity information to an agency application. In addition, this volume offers privacy-enhancing techniques to share information about a valid, authenticated subject and describes methods that allow for strong multi-factor authentication (MFA) while the subject remains pseudonymous to the digital service.

OMB M-07-16: *Safeguarding Against and Responding to the Breach of Personally Identifiable Information, Control Remote Access* states:

> Allow remote access only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access.

OMB M-11-11: ***Continued Implementation of Homeland Security Presidential Directive (HSPD) 12– Policy for a Common Identification Standard for Federal Employees and Contractors*** states:

> Effective immediately, all new systems under development must be enabled to use PIV credentials, in accordance with NIST guidelines, prior to being made operational.
>
> Effective the beginning of FY 2012, existing physical and logical access control systems must be upgraded to use PIV credentials, in accordance with NIST guidelines, prior to the agency using development and technology refresh funds to complete other activities.

Cause:

The EEOC OIT has provided authentication for its digital systems and developed plans to implement multifactor authentication. In June 2017, NIST issued Special Publication 800-63-3 Digital Identity Guidelines, as guidelines for conducting risk assessment and implementation of digital services. The EEOC OIT has not implemented the new NIST SP 800-63-3 requirements. The EEOC OIT has developed a plan for 2017 to implement two-factor authentication for privilege users and a pilot remote logical access program. EEOC OIT plans to implement two-factor authentication for non-privilege users in 2018. Although the EEOC OIT has made progress in developing a plan to implement two-factor authentication, this does not fully satisfy OMB mandates related to two-factor authentication.

Effect:

Not providing the appropriate levels of authentication for digital services, increases the risk of EEOC OIT providing services to the wrong subject (e.g., an attacker successfully proofs as someone else). Using password-base single-factor user authentication places EEOC at risk of an attacker capturing a password by acquiring a password from storage, transmission, or user knowledge and behavior; an attacker guessing a password by repeatedly attempting to authenticate using default passwords, dictionary words, and other likely passwords; an attacker cracking a password offline by recovering cryptographic password hashes and using analysis methods to attempt to identify a character string that will produce one of these hashes; and an attacker resetting an existing password to an attacker-selected password. Multi-factor authentication makes it more difficult for an attacker to gain unauthorized access to a system. An attacker would have to compromise two factors—not just one—to gain access, such as something the user has (a smart card) and either something the user knows (a password or PIN to unlock the smart card) or something the user is (a biometric characteristic to unlock the smart card)[3].

[3] NIST *Best Practices for Privileged User PIV Authentication, Limitations of Password-Based Single-Factor Authentication*, page 1. https://csrc.nist.gov/csrc/media/publications/white-paper/2016/04/21/best-practices-for-privileged-user-piv-authentication/final/documents/best-practices-privileged-user-piv-authentication.pdf

Recommendation 3

We recommend the EEOC OIT conduct an e-authentication risk assessment based on NIST SP 800-63-3 *Digital Identity Guidelines* suite, for EEOC's digital services, and fully implement multifactor authentication for logical and remote access enterprise-wide.

Management's Response:

EEOC's management provided the following response to the finding and recommendation:

> *OIT concurs with the recommendation. We have implemented multifactor authentication (MFA) using EEOC's Personal Identity Verification (PIV) cards within a test environment and will be piloting PIV-based MFA for privileged users during the first quarter of FY 2018. OIT will work with the Office of the Chief Financial Officer and Office of Field Programs to initiate implementation of PIV-based MFA enterprise-wide during the fiscal year. OIT will also conduct new e-authentication risk assessments against the recently updated NIST SP 800-63-3 guidance during FY 2018.*

Auditor's Evaluation of Management's Response

EEOC's management concurred with the recommendations.

Management's full response is provided in **Appendix C**.

Finding 4:	**Separation of Duties between the Chief Information Security Officer (CISO) and Deputy Chief Information Officer (DCIO) Positions.**

Condition:

The EEOC DCIO serves as the CISO for the Office of Information and Technology. The dual roles create a conflict between the DCIO's and CISO's responsibilities to manage EEOC's Information Security Program and information system security risks. In this capacity, the DCIO is responsible for all aspects of the Information Resources Management (IRM) and Information Technology (IT) Program relating to strategic planning, budget, capital asset planning, policy development, information security, project management, and quality assurance.

As stated in the position description for the DCIO, "the Chief Information Officer (CIO) exercises administrative supervision over the DCIO. Together with the CIO, the DCIO establishes the overall broad goals and objectives of the Information Security Program. The DCIO independently plans, organizes, coordinates, directs, and evaluates the work of the program, referring to the CIO only policy matters. The DCIO's final work products and/or findings, decisions, and recommendations are considered technically authoritative. The CIO's review is only to determine the effectiveness of dealing with management and program issues and problems which may arise."

The CISO, also known as the Senior Agency Information Security Officer, was established under the Federal Information Security Modernization Act of 2014 (FISMA 2014). The CISO[4] establishes, implements, and maintains the organization's Information Security Continuous Monitoring (ISCM) Program; develops organizational program guidance (i.e., policies/procedures) for continuous monitoring of the security program and information systems; develops configuration management guidance for the organization; consolidates and analyzes Plan of Action and Milestones (POA&Ms) to determine organizational security weaknesses and deficiencies; acquires or develops and maintains automated tools to support ISCM and ongoing authorizations; provides training on the organization's ISCM program and process; and provides support to information owners/information system owners and common control providers on how to implement ISCM for their information systems.

The CISO responsibilities include knowing where the critical data is located, what the EEOC's risk threshold is should the data become compromised, and how to protect this data while supporting the business' objectives. The CISO is instrumental in defining and implementing EEOC's risk management framework to properly govern, evaluate, and respond to risks involving the EEOC's protected data. The CISO is also heavily involved in vendor risk management (VRM) of the EEOC's third and fourth parties—for example, ensuring critical data is only accessible to those who need access to perform required tasks.

The responsibilities of the CISO conflict with the responsibilities of the DCIO. The CISO role frequently requires decisions to reject what they consider unnecessary business risks—so the DCIO simply may overrule the CISO decision-making process. With the rise of cybercrime and the evolving threat landscape, this scenario should be avoided. The CISO should have a firm grasp on how to report on the risk environment both holistically and within the agency in order to give the board of directors the information it needs to make decisions.

The EEOC OCIO should separate the DCIO and CISO position in order to avoid the conflict of duties when reporting to the CIO. The OCIO needs the additional resources to improve the information system security program maturity level from "Consistently Implemented" to "Managed and Measurable" for the following: (1) Protect (Identity and Access Management) and (2) Respond (Incident Response)[5].

Criteria

The Clinger-Cohen Act, FISMA, and FITARA established responsibilities for Chief Information Officer, which are delegated to the DCIO.

Clinger-Cohen Act (40 U.S.C. §§ 11101-11704) states: 44 U. S. C. § 3506 (Clinger-Cohen Act)

> (b) GENERAL RESPONSIBILITIES.—The Chief Information Officer of an executive agency shall be responsible for—

[4] The NIST's "Role of an Organizational Information Security Continuous Monitoring (ISCM) Program" provides a description of the CISO roles related the ISCM.
[5] FY 2017 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics V 1, April 17, 2017

(1) providing advice and other assistance to the head of the executive agency and other senior management personnel of the executive agency to ensure that information technology is acquired and information resources are managed for the executive agency in a manner that implements the policies and procedures of this division, consistent with chapter 35 of title 44, United States Code, and the priorities established by the head of the executive agency;
(2) developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture for the executive agency; and (3) promoting the effective and efficient design and operation of all major information resources management processes for the executive agency, including improvements to work processes of the executive agency.

The Federal Information Security Modernization Act of 2014 (FISMA 2014) Public Law 113–283—DEC. 18, 2014, states:

"§ 3554. Federal agency responsibilities

"(a) IN GENERAL.—The head of each agency shall—
"(3) delegate to the agency Chief Information Officer established under section 3506 (or comparable official in an agency not covered by such section) the authority to ensure compliance with the requirements imposed on the agency under this subchapter, including—
"(A) designating a senior agency information security officer who shall—
"(i) carry out the Chief Information Officer's responsibilities under this section;
"(ii) possess professional qualifications, including training and experience, required to administer the functions described under this section;
" (iii) have information security duties as that official's primary duty; and
"(iv) head an office with the mission and resources to assist in ensuring agency compliance with this section;
"(B) developing and maintaining an agencywide information security program as required by subsection (b);
"(C) developing and maintaining information security policies, procedures, and control techniques to address all applicable requirements, including those issued under section 3553 of this title and section 11331 of title 40;
"(D) training and overseeing personnel with significant responsibilities for information security with respect to such responsibilities; and
"(E) assisting senior agency officials concerning their responsibilities under paragraph (2).

The Federal Information Technology Acquisition Reform Act (FITARA), enacted in December 2014, imposes new requirements on Federal agencies for transparency and accountability for how IT is planned and implemented in the Federal government. The law requires EEOC and other Federal agencies to strengthen the Chief Information Officer's (CIO) role in

overseeing IT investments and ensuring the alignment of IT investments with Agency strategic business objectives.

Cause

The DCIO serves as CISO because the agency does not have adequate resources fill the CISO position.

Effect

The effect of both positions (DCIO and CISO) reporting to the CIO increased the risk of conflict in fulfilling the responsibilities of the DCIO and CISO.

Recommendation 4

We recommend that EEOC establish a separate position for the Deputy Chief Information Security Officer and Chief Information Security Officer (CISO) as additional resources to meet Federal information system security program requirements and reduce the risk of conflict in managing operations and security risk.

Management's Response

OIT concurs with the recommendation and has included the necessary new position as a top priority in recent hiring requests.

Auditor's Evaluation of Management's Response

EEOC's management concurred with the recommendations.

Management's full response is provided in **Appendix C**.