10. Appendix C – EEOC Management's Comments

U.S. EQUAL EMPLOYMENT OPPORTUNITY COMMISSION
Washington, D.C. 20507

February 7, 2019

MEMORANDUM

TO: Milton Mayo, Inspector General

FROM: Jamell Fields, Chief Information Security Officer

Digitally signed by JAMELL FIELDS
DN: c=US, o=U.S. Government, ou=Equal Employment Opportunity Commission, cn=JAMELL FIELDS, 0.9.2342.19200300.100.1.1=45001003673996
Date: 2019.02.07 16:34:37 -05'00'

SUBJECT: Office of Information Technology's (OIT) Response to the FY 2018 Independent Evaluation of the EEOC's Compliance with Provisions of the Federal Information Security Modernization Act (FISMA)

Below are OIT's responses to the draft findings and recommendations outlined in the above referenced evaluation. Please feel free to contact me at jamell.fields@eeoc.gov or 202.663.4446 if you have any questions related to our responses.

FINDING/RECOMMENDATIONS:

1. **Finding: The Office of Information (OIT) has not employed an automated mechanism that ensures full-encryption of sensitive data and Personally Identifiable Information (PII) on mobile devices.**

   Recommendation 1: We recommend the OIT employ an automated mechanism that ensures sensitive PII (SPII) is encrypted on removable mobile media.

   Response: The audit finding specifically references that EEOC cannot prevent users from storing unencrypted sensitive and PII data on untrusted portable devices, such as USB drives. OIT intends to further implement the data loss prevention (DLP) controls within its Office 365 subscriptions, bolstered by the deployment of Windows 10, to better protect sensitive data from exfiltration.

   OIT also is in the process of implementing secure repositories for sensitive data within SharePoint, including for the purposes of receiving and sharing this data with external parties. These repositories include DLP policies to monitor and automatically protect sensitive information, including implementing controls that regulate the download of sensitive data. The use of secure SharePoint repositories and mission focused electronic services will greatly diminish the need to use removable media to transport sensitive data.

   By improving data safeguards and reducing the need to use removable media, OIT believes it can resolve the finding and improve the services provided to the program offices.

Office of Information Technology
Phone (202) 663-4447 | FAX (202) 663-4451 | TTY (202) 663-7193 | Help Desk (202) 663-4767

2. **Finding: The Office Chief Human Capital Officer (OCHCO) and OIT need to conduct a baseline assessment of the EEOC's cybersecurity workforce.**

   Recommendation 2: We recommend the OCHCO and OIT define and implement a process for conducting an assessment of the knowledge, skills, and abilities of EEOC's cybersecurity workforce.

   Recommendation 3: We recommend the OCHCO and OIT conduct a baseline assessment of the EEOC's cybersecurity workforce that includes (1) the percentage of personnel with IT, cybersecurity, or other cyber-related job functions who hold certifications; (2) the level of preparedness of other cyber personnel without existing credentials to take certification exams; and (3) a strategy for mitigating any gaps identified with appropriate training and certification for existing personnel.

   Response: OIT will partner with OCHCO to ensure EEOC compliance with the Federal Cybersecurity Workforce (CSWF) Act of 2015. EEOC will evaluate current position descriptions (PD) for existing OIT personnel and assess against current role requirements while considering the National Initiative for Cybersecurity Education (NICE) framework. This framework will support by providing a common lexicon and proper taxonomy to define the cybersecurity work as well as the requirements that aligns to the role.

3. **Finding: The OIT needs to analyze and resolve internal vulnerabilities.**

   Recommendation 4: We recommend the OIT review and remediate critical-risk, high-risk and moderate-risk vulnerabilities. These vulnerabilities should be resolved to avoid compromise to EEOC's systems; or the Agency should document acceptance of the risk or reclassification of the risk.

   Response: OIT concurs with this finding and recommendation. OIT will (1) evaluate current vulnerability remediation lifecycles as well as scenarios which affect this lifecycle; (2) explore vulnerability management timelines and remediation procedure methodologies; and (3) draft, approve and implement improved vulnerability management standard operating procedures (SOP).

cc: Bryan Burnett, CIO
Pierrette McIntire, DCIO
Greg Frazier, OIG