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

Office of Inspector General

March 24, 2021

MEMORANDUM

TO: Charlotte A. Burrows
Chair

Bryan Burnett
Chief Information Officer

FROM: Milton A. Mayo Jr.
Inspector General

SUBJECT: Final Report: Performance Audit of the U.S. Equal Employment Opportunity Information Security Modernization Act of 2014 (FISMA) For Fiscal Year 2020 (OIG Report Number 2020-003-AOIG)

The Office of Inspector General (OIG) contracted with the independent certified public accounting firm of Harper, Rains, Knight & Company, P.A. (HRK) to conduct a performance audit of EEOC's information security program and practices in accordance with the Federal Information Security Modernization Act of 2014 (FISMA). The contract required HRK conduct the audit in accordance with U.S. generally accepted government auditing standards (GAGAS) contained in *Government Auditing Standards*, issued by the Comptroller General of the United States.

The objective of this performance audit was to assess the effectiveness of the EEOC's information security program and practices for the period October 1, 2019 through September 30, 2020. HRK found that while EEOC has established and maintained an effective information security program and practices, consistent with applicable guidance, HRK found that EEOC's Office of Information Technology (OIT) needs to remediate internal vulnerabilities on its network. HRK recommended EEOC review and remediate critical-risk and high-risk vulnerabilities in accordance with EEOC OIT's assessment of risk. Where risk acceptance is required for vulnerabilities based on EEOC's network operation, HRK recommended that EEOC formally document the risk acceptance along with any associated mitigation activities. EEOC's management was given the opportunity to review the draft report. They agreed with the recommendation and their comments are included in the report in Appendix B.

The OIG does not express an opinion on EEOC's FISMA audit or conclusions about the effectiveness of security program and practices, or conclusions on compliance with laws and other matters. HRK is responsible for the attached auditors' report dated February 24, 2021, and the conclusions expressed therein.

The Office of Management and Budget issued Circular Number A-50, Audit Follow-up, to ensure that corrective action on audit findings and recommendations proceed as rapidly as possible. EEOC Order 192.002, Audit Follow-Up Program, implements Circular Number A-50 and requires that for resolved recommendations, a corrective action work plan should be submitted within 30 days of the final audit

report date describing specific tasks and completion dates necessary to implement audit recommendations. Circular Number A-50 requires prompt resolution and corrective action on audit recommendations. Resolutions should be made within six months of final report issuance.

cc: Mona Papillon
Acting Chief Operating Officer

Elizabeth Fox-Solomon
Chief of Staff

Bryan Burnett
Chief Information Officer

Pierrette McIntire
Deputy Chief Information Officer

Jamell Fields
Chief Information Security Officer

Donnie Landon,
Audit Follow-Up Coordinator