Report in Brief
Date: March 31, 2023
Report No. A-18-22-11200

U.S. DEPARTMENT OF HEALTH & HUMAN SERVICES
OFFICE OF INSPECTOR GENERAL

Why We Did This Audit

The Federal Information Security Modernization Act of 2014 (FISMA) requires Inspectors General to perform an annual independent evaluation of their agency's information security programs and practices to determine the effectiveness of those programs and practices. HHS OIG engaged Ernst & Young LLP (EY) to conduct this audit.

EY conducted a performance audit of HHS' compliance with FISMA as of September 30, 2022, based upon the FISMA reporting metrics defined by the Inspectors General.

Our objective was to determine whether HHS' overall information technology security program and practices were effective as they relate to Federal information security requirements.

How We Did This Audit

We reviewed applicable Federal laws, regulations, and guidance; gained an understanding of the current security program at the Department level and the security programs at 4 of the 12 operating divisions (OpDivs); assessed the status of HHS' security program against the Department and selected OpDivs' information security program policies, other standards and guidance issued by HHS management, and prescribed performance measures; inquired of personnel to gain an understanding of the FISMA reporting metric areas; inspected selected artifacts, and conducted procedures on prior year issues.

Review of the Department of Health and Human Services' Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2022

What We Found

Overall, through the evaluation of FISMA metrics, it was determined that the HHS' information security program was 'Not Effective'. This determination was made based on HHS not meeting the 'Managed and Measurable' maturity level for the Core Inspector General metrics in the function areas of Identify, Protect, Detect, Respond, and Recover. Overall, HHS remains in a similar position to their previously evaluated maturity level. The Department is aware of opportunities to strengthen their overall information security program. HHS has continued to implement changes that support progress towards improved maturity of their enterprise-wide cybersecurity program across all FISMA domains. HHS continues to define and update policies that are distributed to OpDivs to assist with their own policy definitions or to guide consistent implementation of a compliant cybersecurity strategy. We have identified a number of areas that would strengthen the Department's overall information security program.

What We Recommend and HHS Comments

We made recommendations to the Office of the Chief Information Officer that should further strengthen HHS's cybersecurity program and enhance information security controls at HHS. Recommendations specific to deficiencies found at the reviewed HHS OpDivs were provided separately.

HHS should commit to implementing recommendations identified within this report and incorporate enhancements into the overall formal Cybersecurity Maturity Strategy that allows HHS to continue to advance its cybersecurity program from its current maturity state to Managed and Measurable or to the maturity level that HHS deems as effective for their environment, in agreement with the OIG. HHS' information security program should address gaps between the current maturity levels to the appropriate effective maturity level for each function area. HHS should ensure that policies and procedures are being consistently implemented as defined across all OpDivs in order to meet the requirements for effective maturity. This oversight should extend to all requirements whether they are to be implemented using centralized, federated, or hybrid controls.

In written comments to our report, HHS concurred with our Department, Op-Div, and enterprise 1 and 2 recommendations; while not concurring with enterprise recommendations 3 and 4. For the two non-concurrence responses, both were associated with the separation of responsibilities between the HHS OCIO and the OpDivs. While we recognize the federated nature of the HHS environment, responsibility for OCIO to provide oversight of the OpDivs still exists which is why we recommended that OCIO work with the OpDivs to confirm appropriate controls are in place. We maintain that our recommendations are still valid.