Report in Brief
Date: April 2021
Report No. A-18-20-11200

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

Review of the Department of Health and Human Services' Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2020

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, 2020 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 HHS and 5 out of the 12 operating divisions (OpDivs); assessed the status of HHS' security program against HHS 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; and inspected selected artifacts.

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 (1) the evaluation of HHS not meeting a 'Managed and Measurable' maturity level for Identify, Protect, Detect, Respond, and Recover function areas, (2) the deficiencies within the Identify, Protect and Respond function areas and (3) the evaluation of a maturity level below Consistently Implemented for some FISMA metric questions both at HHS overall and at selected operating divisions (OpDivs). However, HHS continues to implement changes to strengthen the maturity of its enterprise-wide cybersecurity program. Progress continues to be made to sustain cybersecurity maturity across all FISMA domains. Also notable were increased maturation of data protection and privacy and information systems continuous monitoring. Weaknesses continue to persist in Contingency Planning, which was the only domain assessed with a maturity level of "Defined" in FY 19 and again in FY 20. We identified opportunities where HHS can strengthen its overall information security program.

What We Recommends and HHS Comments

We recommend that HHS further strengthen its cybersecurity program and enhance information security controls at HHS. Recommendations specific to a reviewed HHS OpDiv were provided to them separately.

HHS should commit to implementing the results of the pilot HHS-wide risk assessment into a formal Cybersecurity Maturity Migration 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. HHS' program should address gaps between the current maturity levels to the HHS-defined effective maturity level for each cybersecurity framework function areas. Roles and shared responsibilities should be articulated and implemented to meet the requirements for effective maturity, including whether requirements are to be implemented using centralized, federated, or hybrid controls.

In written comments to our draft report, HHS concurred with 11 recommendations and did not concur with two recommendations. HHS also provided technical comments, which we addressed as appropriate. We maintain that our findings and recommendations are accurate and valid.