Report in Brief
Date: April 2022
Report No. A-18-21-11200

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 2021

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, 2021, 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 5 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; 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 HHS not meeting the 'Managed and Measurable' maturity level for the Identify, Protect, Detect, Respond, and Recover function areas as required by DHS guidance and the FY 2021 Inspector General FISMA Reporting Metrics. 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. HHS is aware of opportunities to strengthen the Department's overall information security program which would help ensure that all OpDivs are consistently implementing and in line with the requirements across their security programs. We identified opportunities where HHS can strengthen its 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 also 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, in agreement with the OIG. HHS' information security program should address gaps between the current maturity levels to the deemed effective maturity level for each function area. 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.

After issuing our draft report and based on feedback and discussion with HHS prior to HHS providing written comments, we consolidated 3 of our enterprise-wide recommendations into 1 recommendation for an enterprise-wide risk assessment over known control weaknesses in this final report. In written comments to our draft report, HHS concurred with all of our recommendations and described actions it has taken or plans to take to address them. HHS also provided technical comments, which we addressed as appropriate.