Report in Brief
Date: April 2020 Report
No. A-18-19-11200

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 2019

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, 2019 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 selected 4 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, HHS continues to implement changes to strengthen the maturity of its enterprise-wide cybersecurity program. Progress has been made to mature cybersecurity in the Configuration Management and Information Security Continuous Monitoring FISMA domains. Both domains were assessed at Consistently Implemented maturity in FY 2019, an improvement from Defined in FY 2018. Also notable was increased maturation of Incident Response. We identified opportunities where HHS can strengthen its overall information security program. Weaknesses continue to persist in Contingency Planning, which was the only domain assessed as Defined. Additionally, we identified weaknesses in each of the IG FISMA domains: risk management, configuration management, identity and access management, data protection and privacy, security training, information security continuous monitoring, incident response and contingency planning.

What We Recommend and HHS Comments

We recommend that HHS further strengthen its cybersecurity program and enhance information security controls at HHS. Specific recommendations were also provided to the HHS OPDIVs reviewed.

HHS should commit to creating and implementing a Cybersecurity Maturity Migration Strategy to advance the cybersecurity program from its current maturity state to Managed and Measurable across HHS. A progression road map and plan should be developed that includes specific, measurable, attainable, relevant and time-bound (SMART) milestones.

HHS' program should address current gaps between the current maturity levels to the level of Managed and Measurable. 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.

HHS concurred with all of our recommendations. HHS also provided technical comments, which we addressed.

The full report can be found at https://oig.hhs.gov/oas/reports/region18/181911200.asp.