Report in Brief

Date: March 2018
Report No. A-18-17-11200

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

Why We Did This Review

The Federal Information Security Modernization Act of 2014 (FISMA) requires Inspectors General to perform an annual independent evaluation of the information security program and practices of the agency to determine the effectiveness of such programs and practices. OIG engaged Ernst & Young LLP to conduct this review.

We conducted a performance audit of HHS' compliance with FISMA as of September 30, 2017 based upon the questions outlined in the FISMA reporting metrics for the Inspectors General.

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

How We Did This Review

We reviewed applicable Federal laws, regulations, and guidance; gained an understanding of the current security program at HHS and selected operating divisions (OPDIV); assessed the status of HHS' security program against HHS and selected OPDIV 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.

Review of the Department of Health and Human Services' Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2017

What We Found

Overall, HHS has made improvements and continues to implement changes to strengthen its enterprise-wide information security program including adhering to security training procedures and updating policies and procedures. Further, HHS continues to work towards implementing a Department-wide Continuous Diagnostics and Mitigation (CDM) program, coordinating with the Department of Homeland Security (DHS). CDM will allow for HHS to monitor personnel activity, networks, and information systems, as well as report progress through DHS dashboards.

While HHS continue to improve their information security program, opportunities to strengthen the overall information security program were identified which should allow HHS to achieve a higher level of maturity for its information security program. We continued to identify weaknesses in the following areas: risk management, configuration management, identity and access management, security training, information security continuous monitoring, incident response, and contingency planning.

HHS needs to ensure that all OPDIVs consistently review and remediate or address the risk presented by vulnerabilities discovered, consistently implement account management procedures, and accurately track systems to ensure they are operating with a current and valid Authority to Operate. Additionally, the Department should configure newly implemented tools procured from DHS to address program missions and goals and address the root cause for risk, inventory, and continuous monitoring concerns and deficiencies. These steps will strengthen the program and further enhance the HHS mission.

What We Recommend and HHS Comments

We recommend that HHS further strengthen its information security program. We made a series of recommendations to enhance information security controls at HHS and specific recommendations were also provided to the OPDIVs.

HHS concurred with all of our recommendations and described the actions it had taken and plans to take to implement them. HHS also provided technical comments, which we addressed.

The full report can be found at https://oig.hhs.gov/oas/reports/region18/181711200.