Report in Brief

Date: June 2024
Report No. A-18-23-11200

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 2023

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 July 31, 2023, 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 four (4) of the 12 Operating Divisions (OpDivs) and one (1) Staff Division (StaffDiv); 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.

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' inability to meet the "Managed and Measurable" maturity level for the Core and Supplemental Inspector General metrics in the function areas of Identify, Protect, Detect, Respond, and Recover. Overall, the HHS information security program rated ineffective for FY 2023, matching the evaluated program rating from FY 2022. HHS is a federated environment and large disparities continue to exist between the maturity levels at individual OpDivs and StaffDivs. While better performing OpDivs are approaching or at a Managed and Measurable maturity level, certain OpDivs and StaffDiv selected for the audit are either stagnant in their progress towards the Managed and Measurable maturity rating or are regressing and significantly below the Managed and Measurable maturity rating. The Department continues to define and update policies that are distributed to OpDivs and StaffDivs to assist with their own policy definitions or guide consistent implementation of a compliant cybersecurity strategy. However, the Department must go beyond defining and updating policies to achieve the Managed and Measurable level.

What We Recommend

We made recommendations to the Office of the Chief Information Officer to improve its oversight and to enforce accountability to further strengthen HHS's information security program and enhance information security controls at HHS. Recommendations specific to deficiencies found at the reviewed HHS OpDivs and StaffDiv 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 information security program from its current maturity state to Managed and Measurable. HHS should work to ensure that findings are communicated across the organization to increase awareness of identified gaps to help decrease disparity shown across OpDivs and StaffDivs.

In written comments to our report, HHS concurred with our Department and OpDiv recommendations, and enterprise-wide recommendation 3; while not concurring with enterprise-wide recommendations 1, 2, 4, 5, and 6. For two non-concur responses regarding duplicative recommendations, the recommendations are similar but not identical to address weaknesses at the Department and OpDiv levels. For one non-concur related to the repeat of a similar recommendation made in the FY2022 FISMA audit report. The recommendation was removed from this report and the FY2022 recommendation will remain open until addressed. For two non-concur responses, they were associated with the separation of responsibilities between the HHS OCIO and OpDivs. We maintain that our recommendations are valid.