REPORT HIGHLIGHTS

November 2024 | A-18-24-11200

Review of the Department of Health and Human Services' Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2024

Why OIG 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. OIG engaged Ernst & Young LLP (EY) to conduct this audit.
- EY conducted a performance audit of the HHS Chief Information Officer's (HHS's) compliance with FISMA as of July 31, 2024, based upon the 2024 FISMA reporting metrics.
- The audit examined whether HHS's overall information technology security program and practices were effective as they relate to Federal information security requirements.

What OIG Found

Overall, through the evaluation of FISMA metrics, it was determined that HHS's information security program rated "Not Effective" for FY 2024, which is the same as the "Not Effective" program rating from FY 2023.

The determination that HHS's information security program was "Not Effective" was made based on HHS's 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.

What OIG Recommends

We made a series of six recommendations to HHS to strengthen its information security program through improved oversight and information security controls implementation.

HHS concurred with five of our recommendations. HHS did not concur with the recommendation to complete implementation of a cybersecurity risk management strategy, because it believes its current strategy is sufficient.