September 2025 | A-18-22-06100

# Deficiencies With Incorporating Required Cybersecurity Language in HHS Contracts and Timeliness of Contractor Incident Reporting

## Why OIG Did This Audit

- HHS's information and communications technology (ICT) service contractors must report any suspected or confirmed incidents or breaches to HHS.
- A prior Office of Inspector General audit found that some contractors may not be reporting all security incidents to HHS.
- This audit determined whether (1) the contracts that 3 HHS agencies had with 14 selected ICT service contractors included required language about reporting cybersecurity incidents to HHS and (2) the contractors followed HHS requirements to timely report cybersecurity incidents.

## What OIG Found

- Four of the 14 HHS ICT service contractors that we reviewed reported a total of 10 cybersecurity incidents to HHS; however, 2 of those contractors each failed to report an incident to HHS within the 1-hour timeframe stipulated by their contracts.
- Eight of the 14 HHS ICT service contracts that we reviewed—which were awarded by two HHS agencies— did not include required security language regarding the reporting of all suspected or confirmed cybersecurity incidents and breaches. The remaining six contracts—including four awarded by the third HHS agency—included the required security language.

## What OIG Recommends

We made two recommendations to the HHS Office of the Chief Information Officer (OCIO), including that it implement a step in the procurement process to confirm that ICT service contracts contain all required security language before they are awarded.

HHS OCIO concurred with both of our recommendations.