Department of Health and Human Services
Office of Inspector General
Office of Audit Services

September 2025 | A-18-22-06100

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

REPORT HIGHLIGHTS

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.

TABLE OF CONTENTS

INTRODUCTION 1

Why We Did This Audit 1

Objective 1

Background 1

HHS Office of the Chief Information Officer 1

HHS Information and Communication Technology Service Contractors 1

Cybersecurity Incident Reporting Requirements 2

How We Conducted This Audit 2

FINDINGS 3

Two HHS Information and Communications Technology Service Contractors for the Selected Contracts We Reviewed Did Not Promptly Report All Cybersecurity Incidents Within 1 Hour of Identification 3

Eight HHS Information and Communications Technology Service Contracts We Reviewed Did Not Include Required Security Language Regarding the Reporting of All Suspected or Confirmed Cybersecurity Incidents and Breaches 4

RECOMMENDATIONS 5

HHS OFFICE OF THE CHIEF INFORMATION OFFICER COMMENTS 5

APPENDICES

A: Audit Scope and Methodology 7

B: Federal Requirements 9

C: HHS Office of the Chief Information Officer Comments 11

INTRODUCTION

WHY WE DID THIS AUDIT

The Department of Health and Human Services (HHS) contracts with information and communications technology (ICT) service contractors to support HHS operations and assets, including processing, transmitting, and storing HHS data. These ICT service contractors must report all suspected or confirmed information security and privacy incidents to HHS.

By reporting incidents, contractors help to ensure HHS protects against and appropriately responds to cyber threats and adverse events involving HHS systems and data.[1] A prior Office of Inspector General audit found that service contractors may not be reporting all security incidents to HHS.[2]

OBJECTIVE

Our objective was to determine whether HHS ICT service contractors identified and promptly reported cybersecurity incidents in accordance with their information technology (IT) service contracts.

BACKGROUND

HHS Office of the Chief Information Officer

Within the HHS Office of the Secretary, the Office of the Chief Information Officer (OCIO) leads the development and implementation of enterprise IT infrastructure across HHS. Among other responsibilities, OCIO establishes and provides support for IT operations management, IT investment analysis, cybersecurity and privacy, performance measurement, and policies to provide improved management of information resources and technology.

HHS Information and Communications Technology Service Contractors

For Federal fiscal years 2021 through 2023, HHS spent nearly $15.9 billion on ICT service contracts. Among other services, contractors provided services related to IT management, maintenance and support, systems engineering, security and compliance, and network and storage services.

[1] Adverse events are events with a negative consequence, such as system crashes, unauthorized use of system privileges, unauthorized access to sensitive data, and execution of malware that destroys data.

[2] Key findings from the report (A-18-17-04002) are described in OIG's 2022 Top Unimplemented Recommendations: Solutions to Reduce Fraud, Waste, and Abuse in HHS Programs, pg. 36.

Cybersecurity Incident-Reporting Requirements

The *HHS Policy for Information Technology Procurements—Security and Privacy Language* requires that HHS use standard security and privacy language for information and IT contracts. The procurements must use language that requires contractors to report all suspected or confirmed information security and privacy incidents and breaches to HHS as soon as possible and without unreasonable delay, no later than 1 hour. Additionally, procurements must require the contractor to ensure that all contractor employees performing under the contract comply with HHS's Rules of Behavior policy. The *HHS Policy for Rules of Behavior for Use of Information and IT Resources* requires contractors granted access to HHS or Operating Division (OpDiv) information resources and IT systems to report all suspected and identified information security incidents and privacy breaches as soon as possible, without unreasonable delay and no later than 1 hour of occurrence/discovery.

See Appendix B for a summary of Federal cybersecurity incident reporting requirements.

HOW WE CONDUCTED THIS AUDIT

To accomplish our objective, we selected a nonstatistical sample of three HHS OpDivs. We used OIG's Contract & Grants Analytics Portal tool to identify ICT service contracts that these three OpDivs entered into between January 1, 2021, and May 1, 2022, that included services for "information technology and telecommunications." Our list identified 416 total ICT service contracts. From this list, we selected a nonstatistical sample of 14 ICT service contracts with a period of performance that had not expired.[3] Each of the 14 selected ICT service contracts were associated with a different contractor. We reviewed the cybersecurity incidents reported by the 14 ICT service contractors to their respective HHS OpDiv from January 1, 2021, through December 31, 2023.

Our audit work focused on each contractor's reporting requirements, the roles and responsibilities of the associated Contracting Officer's Representatives (CORs) and the Contracting Officers in ensuring a contractor's compliance with the contract's reporting of incident requirement, the contractor's self-reporting of incidents, and the OpDivs' reliance on contractors' self-reporting during the associated contract's period of performance.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix A describes our audit scope and methodology.

[3] The 14 ICT service contracts included 5 from each of 2 OpDivs and 4 from 1 OpDiv.

FINDINGS

Of the 14 ICT service contracts that we reviewed:

- Four HHS ICT service contractors reported 10 cybersecurity incidents; however, 2 of these contractors did not report an identified cybersecurity incident to their HHS OpDiv point of contact within the 1-hour timeframe stipulated by their contracts.

- Eight of the ICT service contracts did not include required language regarding the reporting of all suspected or confirmed cybersecurity incidents and breaches.

These findings occurred because (1) 2 of the 14 selected ICT service contractors did not follow incident-reporting protocols detailed in their contracts with HHS and (2) the procurement process at two of the three OpDivs that we reviewed failed to consistently ensure that the applicable security language used in the contract was correctly included, compliant with, and as restrictive as the security language set forth in the *HHS Policy for Information Technology Procurements - Security And Privacy Language*.

As a result, HHS may not have been aware of incidents or breaches of a contractor's system and not provided an early opportunity to take action to mitigate potential risk to HHS. Additionally, the omission of the required information security contract language for the reporting of all suspected and confirmed incidents and breaches in the awarded contracts could impact OpDivs' and HHS's ability to hold a vendor accountable for meeting HHS requirements for reporting incidents and protect the Government's interests.

TWO HHS INFORMATION AND COMMUNICATIONS TECHNOLOGY SERVICE CONTRACTORS FOR THE SELECTED CONTRACTS WE REVIEWED DID NOT PROMPTLY REPORT ALL CYBERSECURITY INCIDENTS WITHIN 1 HOUR OF IDENTIFICATION

HHS Policy for Information Security and Privacy Protection (IS2P) requires all organizations conducting business on behalf of HHS to report suspected incidents as soon as possible and without unreasonable delay. Also, as required in the *HHS Policy for Information Technology Procurements – Security and Privacy Language,* the terms and conditions of HHS's contracts with ICT contractors specifies a 1-hour time frame for reporting incidents and breaches to HHS government officials.[4] The COR is responsible for ensuring the contractor adheres to the terms and conditions of HHS's contracts regarding the reporting of incidents.

From January 1, 2021, through December 31, 2023, 4 of 14 selected HHS ICT service contractors reported a total of 10 cybersecurity incidents to HHS. Of these four HHS ICT service

[4] "HHS government officials" specified in the *HHS Policy for Information Technology Procurements - Security and Privacy Language* include, but are not limited to, the OpDiv's Incident Response Team, COR, Contracting Officer, and Senior Official for Privacy.

contractors, two did not promptly report one cybersecurity incident each to HHS government officials within 1 hour of identification. Specifically:

- One ICT service contractor reported a cybersecurity incident involving an IT system's internal disclosure of the first name of system users' accounts 1 day after an authorized user observed the incident. Also, the contractor was required to report incidents to a point of contact designated in their contract; however, the contractor initially reported the incident to an OpDiv official rather than the point of contact designated in their contract to receive reports of such incidents.

- One ICT service contractor reported a suspected cybersecurity incident involving unauthorized access from screen-sharing by a remote user about 10 hours after the contractor was unable to confirm or refute the event. Specifically, the contractor's staff member initially reported to their project manager, who then was unable to confirm or refute the suspected security incident. The contractor reported the activity as a security incident to the proper OpDiv point of contact listed in its contract.

These delays occurred because the selected ICT service contractors did not follow incident-reporting protocols detailed in their contracts with HHS. For one of the instances identified above, the contractor's confusion over its incident-reporting protocol contributed to its delay in reporting the incident to the OpDiv. As a result, HHS may not have been aware of the incident or breach of the contractor's system and not provided an early opportunity to take action to mitigate potential risk to HHS.

EIGHT HHS INFORMATION AND COMMUNICATIONS TECHNOLOGY SERVICE CONTRACTS WE REVIEWED DID NOT INCLUDE REQUIRED SECURITY LANGUAGE REGARDING THE REPORTING OF ALL SUSPECTED OR CONFIRMED CYBERSECURITY INCIDENTS AND BREACHES

HHS Policy for Information Technology Procurements - Security and Privacy Language states that, for contracts that involve a procurement requiring information security, the contract must include the following language: "In the event of a suspected or confirmed incident or breach, the Contractor (and/or any subcontractor) must … [r]eport all suspected and confirmed information security and privacy incidents and breaches." Additionally, the policy states that it is the responsibility of the OpDiv's Contracting Officer to make sure all applicable security and privacy language is included in the contract. The policy further prescribes for the requiring activity representative and contracting office,[5] the OpDiv Information System Security Officer (ISSO), Senior Official for Privacy (SOP), System Owner and the Chief Information Security Officer (CISO), to ensure procurement documentation includes the appropriate contract security language and identify any additional security language applicable to the contract. In addition, the policy sets forth the procedures, and an IT Information Security & Privacy Certification Checklist, to help ensure all applicable security language is included in contracts.

[5] HHS defines the requiring activity as a group or individual responsible for defining the acquisition requirements needed to assist HHS in completing a duty or task.

Further, the policy requires OpDivs' IT procurement contract language to remain compliant with and as restrictive as the security language and requirements specified in the policy.

Of the 14 selected ICT service contracts, 6 correctly included language requiring the contractor to report all suspected or confirmed cybersecurity incidents and breaches. The remaining eight contracts lacked this language. Specifically, five of these contracts, associated with one OpDiv, only required reporting of incidents and breaches involving unsecured protected health information. The other three contracts, associated with another OpDiv, required reporting only for suspected or confirmed breaches.

The procurement process at the selected OpDivs failed to consistently ensure that the applicable security language used in the contract was correctly included, compliant with, and as restrictive as the security language set forth in the *HHS Policy for Information Technology Procurements - Security and Privacy Language*. As a result, contractors only reported what was required by their ICT service contract and OpDiv. The omission of the required information security contract language for the reporting of all suspected and confirmed incidents and breaches in the awarded contract could impact OpDivs' and HHS's ability to hold a vendor accountable for meeting HHS requirements for reporting incidents and to protect the Government's interests.

RECOMMENDATIONS

We recommend that the Department of Health and Human Services Office of the Chief Information Officer:

- require OpDivs to modify any ICT service contracts that lack required security language, including the required language as stated in the *HHS Policy for Information Technology Procurements – Security and Privacy Language*, and

- implement a verification step in the procurement process to confirm that all ICT service contracts include the required security language pertaining to incident reporting before awarding the contracts.

HHS OFFICE OF THE CHIEF INFORMATION OFFICER COMMENTS

In written comments on our draft report, HHS OCIO concurred with both of our recommendations and described actions it has taken to respond to our first recommendation.

Regarding our first recommendation, HHS OCIO stated that security and privacy language standards set by OCIO in the *HHS Policy for Information Technology Procurements - Security and Privacy Language* were converted to the HHS Acquisition Regulation as standardized contract language. HHS OCIO stated that this was done to reduce inconsistencies in how

HHS Divisions were applying applicable security and privacy language in Divisions' solicitations and contracts.

HHS OCIO concurred with our second recommendation and stated that reviews and verification of the required security language pertaining to incident reporting already takes place at several points in the acquisition process.

HHS OCIO's comments are included as Appendix C.

APPENDIX A: AUDIT SCOPE AND METHODOLOGY

SCOPE

Our audit covered ICT service contractors' reporting of identified cybersecurity incidents to HHS from January 1, 2021, through December 31, 2023. We selected a nonstatistical sample of 14 ICT service contracts, with a current period of performance that had not expired, out of 416 total ICT service contracts from 3 nonstatistically selected OpDivs. Each of the 14 ICT service contracts were associated with a different contractor, for a total of 14 ICT service contractors.

We conducted interviews with HHS's Computer Security Incident Response Center (CSIRC); HHS's Computer Security Incident Response Team (CSIRT); staff at the three selected OpDivs, CORs, and Contracting Officers; and contractors' staff and contract project managers to gain an understanding of the roles and responsibilities involved in contractors' reporting of cybersecurity incidents. We reviewed HHS and OpDivs' cybersecurity incident reporting documentation, HHS policies governing contractors' reporting of cybersecurity incidents, and IT acquisition contract requirements for reporting cybersecurity incidents.

During our audit work, we obtained from HHS CSIRT an HHS CSIRC-generated incident ticket report. However, HHS CSIRC's incident management tool was not able to identify the business name of a contractor from the tool's incident-tracking tickets and reports. Therefore, our audit work required us to correlate and track incident ticket-reporting at the OpDiv level.

We assessed the departmental controls over incident-reporting and OpDivs' controls over contractors' incident-reporting. Our audit covered the requirements in ICT service contracts for the reporting of security incidents and the mandated standard security contract language for IT procurements. We interviewed individuals with knowledge of and responsibilities associated with incident reporting within HHS, which included staff at HHS CSIRC, HHS CSIRT, and the selected OpDivs (e.g., CORs and Contracting Officers); and contractors' staff, contract project managers and leads.

We did not assess HHS's and the selected OpDivs' overall internal controls. Rather, we limited our review of internal controls to those applicable to our audit objective. Specifically, we examined HHS's and OpDivs' policies, procedures, and internal practices applicable to ICT contractors reporting of incidents to HHS and HHS OpDivs.

We conducted our audit work from April 2022 through July 2025.

METHODOLOGY

To accomplish our objective, we:

- reviewed Federal requirements and OpDivs' policies related to reporting incidents;

- selected a nonstatistical sample of 14 ICT service contracts, with a current period of performance that had not expired, from 3 nonstatistically selected OpDivs and, for each ICT service contract, reviewed the ICT service contract and the statement of work or performance work statement, between the contractor and the OpDiv;

- reviewed the required responsibilities of the COR, as documented in the OpDivs' COR appointment memorandum letters for each of the 14 ICT service contracts;

- examined incidents reported to HHS CSIRC by the selected OpDivs to determine whether contractors reported security incidents to the HHS OpDivs;

- examined incident tracking tickets and reports of incidents reported to the selected OpDivs by the contractor associated with each of the 14 ICT service contracts to determine whether the contractor reported security incidents timely;

- interviewed CSIRC, OpDiv, and contractor personnel to gain an understanding of their policies and procedures for reporting incidents; and

- discussed the results of our audit with HHS and OpDiv officials.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for the findings and conclusions based on our audit objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

APPENDIX B: FEDERAL REQUIREMENTS

DEPARTMENT OF HEALTH AND HUMAN SERVICES POLICIES

HHS Policy for Information Security and Privacy Protection (IS2P)

HHS IS2P policy states that this policy applies to all OpDivs, staff divisions, and organizations conducting business for, and collecting, processing or maintaining information or using or operating systems on behalf of, the Department, whether directly or through contractual relationships.

Section 7.38. All Users (system user) states users must notify the OpDiv CISO or OpDiv CSIRT of actual or suspected computer security-related incidents, anomalous or suspicious system behavior, and all suspected or confirmed personally identifiable information and protected health information breaches, including computer-related, paper-based, and verbal breaches.

HHS IS2P security control IR-6 Incident Reporting requires personnel to report suspected incidents to the OpDiv CSIRT as soon as possible and without unreasonable delay.

HHS Policy for Information Technology Procurements - Security And Privacy Language

HHS Policy for Information Technology Procurements - Security And Privacy Language states that:

- the purpose of this policy is to mandate the standard security and privacy language for IT procurements throughout HHS,

- OpDivs may customize this Policy to include OpDiv specific information, create their own policy, or supplement the standard contract language herein, provided the OpDiv standard contract language is compliant with and is as restrictive as the baseline contract language,

- all Contractor employees performing on the contract must adhere to the [HHS] Rules of Behavior, and

- the contractor must report all suspected and confirmed information security and privacy incidents and breaches to the OpDiv, as soon as possible and without unreasonable delay, no later than 1 hour.

"Section 6" of the policy states that the Department and OpDivs must implement the following baseline policy requirements and standards in Appendix B of the policy. "Appendix B: Standards" states that procurements requiring information security and involving information and IT must include the standard contract language:

- Incident Response
  b. In the event of a suspected or confirmed incident or breach, the Contractor (and/or any subcontractor) must: ... Report all suspected and confirmed information security and privacy incidents and breaches.

HHS Policy for Rules of Behavior for Use of Information and IT Resources

Appendix D: Forms and Templates, section 1. "Rules of Behavior for General Users" states that, these Rules of Behavior for General Users apply to contractors and any others who are granted access to HHS/OpDiv information resources and IT systems. Users of HHS/OpDiv information, IT resources and information systems must adhere to the following rules:

- 1.1 HHS/OpDiv Information and IT Resources
  K. Report all suspected and identified information security incidents and privacy breaches to the Helpdesk, HHS/OpDiv Computer Security Incident Response Center (CSIRC), or OpDiv Computer Security Incident Response Team (CSIRT), and
- 1.5 Data Protections
  C. Immediately report all suspected and known security incidents, privacy breaches, and suspicious activities to the Helpdesk and/or CSIRC/CSIRT pursuant to HHS/OpDiv incident response policies and/or procedures.

APPENDIX C: HHS OFFICE OF THE CHIEF INFORMATION OFFICER

OFFICE OF THE CHIEF INFORMATION OFFICER
DEPARTMENT OF HEALTH AND HUMAN SERVICES

August 2025
General Comments to OIG's Draft Report, "Deficiencies with Incorporating Required Cybersecurity Language in HHS Contracts and Timeliness of Contractor Incident Reporting" (A-18-22-06100)

The U.S. Department of Health & Human Services (HHS) Office of the Chief Information Officer (OCIO) appreciates the opportunity from the Office of Inspector General (OIG) to review and comment on this draft report.

Recommendation 1: The Department of Health and Human Services Office of the Chief Information Officer should require OpDivs to modify any ICT service contracts that lack required security language, including the required language as stated in the HHS Policy for Information Technology Procurements – Security and Privacy Language.

HHS Response: HHS concurs with OIG's recommendation. Ensuring that ICT service contracts include the required security and privacy language is a collaborative effort among the HHS CIO, HHS CISO, Division CIOs, Division CISOs, ASFR/OA, Contracting Officers, Contracting Officer Representatives, Requiring Activity Representatives, and more. OCIO has the overarching responsibility for establishing the required security and privacy requirements language. In coordination with ASFR/OA, those requirements are then translated into appropriate acquisition policy and guidance (e.g., HHSAR contract clauses, provisions, etc.) But ultimately, it falls on the Division Requiring Activity Representative and Division Contracting Officer, with the assistance of and in consultation with many others, to ensure that the applicable security and privacy language set forth in Appendix B of the Policy is included in their solicitation and contract.

Note that, until March 2024, the applicable security and privacy language standards set by OCIO were found only in Appendix B of the HHS Policy for Information Technology Procurements - Security and Privacy Language. Recognizing that this could lead to inconsistencies in how HHS Divisions were applying these standards, ASFR/OA began efforts to convert the security and privacy language found in Appendix B into standardized contract language in the HHS Acquisition Regulation (HHSAR). This effort began in 2022 and ultimately resulted in a HHSAR Class Deviation 2024-01 Amendment 1, which was issued and effective on March 1, 2024.

hhsar-class-deviation-2024-01.pdf

Recommendation 2: The Department of Health and Human Services Office of the Chief Information Officer should implement a verification step in the procurement process to confirm that all ICT service contracts include the required security language pertaining to incident reporting before awarding the contracts.

1

August 2025
General Comments to OIG's Draft Report, "Deficiencies with Incorporating Required Cybersecurity Language in HHS Contracts and Timeliness of Contractor Incident Reporting" (A-18-22-06100)

HHS Response: HHS concurs with OIG's recommendation; however, there are already several points in the acquisition process where reviews and verification take place:

- **HHS Division-level reviews:** Each Division with delegated acquisition authority will have its own acquisition review processes in place.
- **Information Security & Privacy Certification Checklist for Procurements**: This document is completed at the initial stage of the procurement for all acquisitions involving information and IT products and services. This document helps determine the applicable security and privacy requirements.
- **IT Acquisition Review (ITAR) Program**: IT and IT-related acquisition packages that meet the review thresholds stated in Section 6 of the HHS Policy for Information Technology Acquisition Reviews require Department CIO review and approval obtained through the HHS ITAR process. While the primary purpose of this program is to ensure that HHS conducts its due diligence to manage and maintain oversight and governance over the procurement of IT, therefore contributing to effective planning, budgeting, and execution of IT resources, it is another review layer where missing required contract language can be identified.
    - In addition to the Department-level ITAR Program, there are also programs at the HHS Division level.

Report Fraud, Waste, and Abuse

OIG Hotline Operations accepts tips and complaints from all sources about potential fraud, waste, abuse, and mismanagement in HHS programs. Hotline tips are incredibly valuable, and we appreciate your efforts to help us stamp out fraud, waste, and abuse.

TIPS.HHS.GOV

Phone: 1-800-447-8477

TTY: 1-800-377-4950

Who Can Report?

Anyone who suspects fraud, waste, and abuse should report their concerns to the OIG Hotline. OIG addresses complaints about misconduct and mismanagement in HHS programs, fraudulent claims submitted to Federal health care programs such as Medicare, abuse or neglect in nursing homes, and many more. Learn more about complaints OIG investigates.

How Does It Help?

Every complaint helps OIG carry out its mission of overseeing HHS programs and protecting the individuals they serve. By reporting your concerns to the OIG Hotline, you help us safeguard taxpayer dollars and ensure the success of our oversight efforts.

Who Is Protected?

Anyone may request confidentiality. The Privacy Act, the Inspector General Act of 1978, and other applicable laws protect complainants. The Inspector General Act states that the Inspector General shall not disclose the identity of an HHS employee who reports an allegation or provides information without the employee's consent, unless the Inspector General determines that disclosure is unavoidable during the investigation. By law, Federal employees may not take or threaten to take a personnel action because of whistleblowing or the exercise of a lawful appeal, complaint, or grievance right. Non-HHS employees who report allegations may also specifically request confidentiality.

Stay In Touch

Follow HHS-OIG for up to date news and publications.

 OIGatHHS

 HHS Office of Inspector General

Subscribe To Our Newsletter

OIG.HHS.GOV

Contact Us

For specific contact information, please visit us online.

U.S. Department of Health and Human Services
Office of Inspector General
Public Affairs
330 Independence Ave., SW
Washington, DC 20201

Email: Public.Affairs@oig.hhs.gov