GAO@100

Highlights

Highlights of GAO-21-403, a report to congressional requesters

June 2021

CYBERSECURITY

HHS Defined Roles and Responsibilities, but Can Further Improve Collaboration

Why GAO Did This Study

HHS and the healthcare and public health sector rely heavily on information systems to fulfill their missions, including delivering healthcare-related services and responding to national health emergencies, such as COVID-19. Federal laws and guidance have set requirements for HHS to address cybersecurity within the department and the sector. Federal guidance also requires collaboration and coordination to strengthen cybersecurity at HHS and in the sector.

GAO was asked to review HHS's organizational approach to address cybersecurity. This report discusses HHS's roles and responsibilities for departmental cybersecurity; HHS's roles and responsibilities for healthcare and public health sector cybersecurity; and HHS's efforts to collaborate to manage its cybersecurity responsibilities.

To perform its work, GAO reviewed documentation describing HHS's cybersecurity roles and responsibilities, assessed those responsibilities for fragmentation, duplication, and overlap, and evaluated the department's collaborative efforts against GAO's leading practices for collaboration. GAO also interviewed relevant officials at HHS and CISA, and in the sector.

What GAO Recommends

GAO is making seven recommendations to HHS to improve its collaboration and coordination within the department and the sector. HHS agreed with six of the recommendations and disagreed with one. GAO continues to believe that all recommendations are appropriate.

View GAO-21-403. For more information, contact Jennifer R. Franks at (404) 679-1831 or franksj@gao.gov.

What GAO Found

The Department of Health and Human Services' (HHS) Office of Information Security is responsible for managing department-wide cybersecurity. HHS clearly defined responsibilities for the divisions within that office to, among other things, document and implement a cybersecurity program, as required by the *Federal Information Security Modernization Act of 2014*.

For healthcare and public health critical infrastructure sector cybersecurity, HHS also defined responsibilities for five HHS entities. Among these entities are the Health Sector Cybersecurity Coordination Center, which was established to improve cybersecurity information sharing in the sector, and the Healthcare Threat Operations Center, a federal interagency program co-led by HHS and focused on, among other things, providing descriptive and actionable cyber data. Private-sector partners that receive information provided by the Health Sector Cybersecurity Coordination Center informed GAO that they could benefit from receiving more actionable threat information. However, this center does not routinely receive such information from the Healthcare Threat Operations Center, and therefore is not positioned to provide it to sector partners. This lack of sharing is due, in part, to HHS not describing coordination between the two entities in procedures defining their responsibilities for cybersecurity information sharing. Until HHS formalizes coordination for the two entities, they will continue to miss an opportunity to strengthen information sharing with sector partners.

Further, HHS entities led, or participated in, seven collaborative groups that focused on cybersecurity in the department and healthcare and public health sector. These entities regularly collaborated on cyber response efforts and provided cybersecurity information, guidance, and resources through these groups and other means during COVID-19 between March 2020 and December 2020. In addition, the HHS entities coordinated with the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) to address cyber threats associated with COVID-19. Further, the HHS entities fully demonstrated consistency with four of the seven leading collaboration practices that GAO identified, and partially addressed the remaining three (see table). Until HHS takes action to fully demonstrate the remaining three leading practices, it cannot ensure that it is improving cybersecurity within the department and the healthcare and public health sector.

Extent to Which the Department of Health and Human Services (HHS) Demonstrated Leading Practices for Collaborating

Leading practice	Extent to which the HHS working groups demonstrated the leading practice
Define and track outcomes and accountability	◑ - five groups met this practice
Bridge organizational cultures	● – all seven groups met this practice
Identify leadership	● – all seven groups met this practice
Clarify roles and responsibilities	◑ - six groups met this practice
Include relevant participants in the group	● – all seven groups met this practice
Identify resources	● – all seven groups met this practice
Document and regularly update written guidance and agreements	◑ - six groups met this practice

Source: GAO analysis of HHS documentation. | GAO-21-403