



June 2021

CYBERSECURITY

HHS Defined Roles and Responsibilities, but Can Further Improve Collaboration

GAO@100 Highlights

Highlights of [GAO-21-403](#), a report to congressional requesters

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.

June 2021

CYBERSECURITY

HHS Defined Roles and Responsibilities, but Can Further Improve Collaboration

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

Contents

Letter		1
	Background	7
	HHS Has Clearly Defined Roles and Responsibilities for Managing the Cybersecurity of the Department	16
	HHS Clearly Defined Its Roles and Responsibilities for Supporting HPH Sector Cybersecurity; However, Opportunity for Improving Coordination Exists	22
	HHS Entities Regularly Shared Cybersecurity Information during COVID-19, but Can Further Improve Collaboration	28
	Conclusions	49
	Recommendations for Executive Action	50
	Agency Comments and Our Evaluation	51
Appendix I	Objectives, Scope, and Methodology	55
Appendix II	Department of Health and Human Services' Cybersecurity-Related Information Sharing Products	61
Appendix III	Comments from the Department of Health and Human Services	63
Appendix IV	GAO Contacts and Staff Acknowledgments	68
Tables		
	Table 1: Responsibilities for the Three Office of Information Security Divisions Managing the Department of Health and Human Services' (HHS) Cybersecurity Program, in accordance with <i>Federal Information Security Modernization Act of 2014</i> (FISMA)	19
	Table 2: Roles and Responsibilities of the Department of Health and Human Services (HHS) Entities that Provide Cybersecurity Assistance to the Healthcare and Public Health (HPH) Critical Infrastructure Sector	24
	Table 3: Roles of the Department of Health and Human Services' (HHS) Cybersecurity-Focused Collaborative Groups	

Supporting Cybersecurity Management at the Department and Coordination in the Healthcare and Public Health (HPH) Sector	29
Table 4: Examples of Cybersecurity-related Products Shared by Department of Health and Human Services (HHS) Entities	33
Table 5: Examples of the Department of Health and Human Services' Cybersecurity Collaborative Groups' Actions that were Generally Consistent with the Leading Practices for Collaboration	37
Table 6: Extent to Which the Department of Health and Human Services' Cybersecurity Collaborative Groups Demonstrated Leading Practices for Collaboration	38
Table 7: Goals of Collaborative Groups led by the HHS Office of Information Security and Office of the Assistant Secretary for Preparedness and Response (ASPR)	39
Table 8: Information Sharing Products Used by the Department of Health and Human Services (HHS) Entities to Help Strengthen Cybersecurity within the Department and Healthcare and Public Health (HPH) Critical Infrastructure Sector	61

Figure

Figure 1: Structure of the Department of Health and Human Services (HHS) Office of the Chief Information Officer's Office of Information Security	18
---	----

Abbreviations

ASPR	Assistant Secretary for Preparedness and Response
BARDA	Biomedical Advanced Research and Development Authority
CDC	Centers for Disease Control and Prevention
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
COVID-19	Coronavirus Disease 2019
CSIRC	Computer Security Incident Response Center
DHS	Department of Homeland Security
FBI	Federal Bureau of Investigation
FDA	Food and Drug Administration
FedRAMP	Federal Risk and Authorization Management Program
FISMA	<i>Federal Information Security Modernization Act of 2014</i>
HC3	Health Sector Cybersecurity Coordination Center
HHS	Department of Health and Human Services
HIPAA	<i>Health Insurance Portability and Accountability Act of 1996</i>
HITECH Act	<i>Health Information Technology for Economic and Clinical Health Act</i>
HPH	Healthcare and Public Health
HTOC	Healthcare Threat Operations Center
IT	information technology
NIH	National Institutes of Health
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
ONC	Office of the National Coordinator for Health Information Technology
PPD 21	Presidential Policy Directive 21
TRACIE	Technical Resources, Assistance Center, and Information Exchange

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

June 28, 2021

Congressional Requesters

The Department of Health and Human Services (HHS) and the organizations that make up the Healthcare and Public Health (HPH) critical infrastructure sector rely heavily on information technology (IT) systems to implement their programs and deliver health and healthcare-related goods and services to the public.¹ For example, HHS currently relies on its HHS Protect platform to provide a holistic view of the U.S. healthcare system to guide the nation's response to the Coronavirus Disease 2019 (COVID-19).² HHS also relies on interconnected IT systems to make operational decisions on the delivery of health and social services. These systems, operated by the department and the HPH sector organizations, process critical sensitive data, such as personally identifiable information and protected health information.³

¹The *Critical Infrastructure Protection Act of 2001* defines "critical infrastructure" as systems and assets, whether physical or virtual, so vital to the United States that their incapacity or destruction would have a debilitating impact on security, national economic security, national public health or safety, or any combination of these. 42 U.S.C. §5195c(e). In 2003, the federal government established the Healthcare and Public Health (HPH) sector as a critical infrastructure sector in the United States, recognizing that its security and resilience are essential to national security, the economy, and public health and safety. Since that time, the HPH sector's partnerships with relevant private sector owners, operators, and professional associations and government representatives at the federal, state, and local levels have strengthened.

²HHS Protect is a secure data ecosystem that is intended to facilitate the collection, sharing, and analyzing of near real-time COVID-19 data. It integrates information from more than 200 datasets from federal, state, and local governments and commercial sources.

³Personally identifiable information is any information that can be used to distinguish or trace an individual's identity, such as name, date, place of birth, and Social Security number. It also includes other types of personal information that can be linked to an individual, such as medical, educational, financial, and employment information. The *Health Insurance Portability and Accountability Act of 1996* and its implementing regulations define protected health information as individually identifiable health information and includes information collected from an individual, including demographic information, that 1) is created or received by a health care provider, health plan, employer, or health care clearinghouse; 2) relates to the past, present, or future physical or mental health condition of the an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual; and 3) identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

The *Federal Information Security Modernization Act of 2014* (FISMA) directs all federal agencies, including HHS, to ensure the cybersecurity of their information and information systems.⁴ In addition, *Presidential Policy Directive 21* (PPD 21) requires HHS to lead the coordination of cybersecurity in the HPH sector.⁵ Given the many players involved in cybersecurity management at the department and in supporting the cybersecurity of the HPH sector, deliberate and well-organized coordination and collaboration are essential to ensure that efforts are successful.

Safeguarding federal information systems and those systems supporting our nation's critical infrastructure has been a longstanding GAO concern. We first designated cybersecurity as a government-wide high-risk area in 1997, and expanded the area to include safeguarding the systems supporting our nation's critical infrastructure in 2003.⁶ We further expanded the cybersecurity high-risk area in 2015 to include protecting the privacy of personally identifiable information.⁷

You requested that we review HHS's organizational structure for addressing cybersecurity within the department and the HPH sector organizations. Our specific objectives for this review were to determine the (1) roles and responsibilities that HHS has defined for its entities to manage cybersecurity within the department; (2) roles and responsibilities that HHS has defined for its entities to assist the cybersecurity efforts of HPH sector organizations; and (3) extent to which HHS entities have

⁴The *Federal Information Security Modernization Act of 2014* (FISMA 2014) (Pub. L. No. 113-283, Dec. 18, 2014) largely superseded the *Federal Information Security Management Act of 2002* (FISMA 2002), enacted as Title III, *E-Government Act of 2002*, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002). As used in this report, FISMA refers both to FISMA 2014 and to those provisions of FISMA 2002 that were either incorporated into FISMA 2014 or were unchanged and continue in full force and effect.

⁵White House, *Presidential Policy Directive 21 (PPD 21)*, Critical Infrastructure Security and Resilience (Feb. 12, 2013).

⁶GAO, *High-Risk Series: An Overview*, [GAO-HR-97-1](#) (Washington, D.C.: February 1997); *High-Risk Series: Information Management and Technology*, [GAO-HR-97-9](#) (Washington, D.C.: February 1997); and *High-Risk Series: An Update*, [GAO-03-119](#) (Washington, D.C.: Jan. 2003).

⁷GAO, *High-Risk Series: An Update*, [GAO-15-290](#) (Washington, D.C.: Feb. 11, 2015). For our most recent update on this high-risk area see *High-Risk Series: Dedicated Leadership Needed to Address Limited Progress in Most High-Risk Areas*, [GAO-21-119SP](#) (Washington, D.C.: Mar. 2, 2021).

effectively collaborated to manage their cybersecurity responsibilities, including COVID-19 cyber response efforts.

To address the first and second objectives, we considered a key principle of an effective control environment on management establishing an organizational structure, assigning responsibility, and delegating authority to achieve the entity's objectives.⁸ To determine how HHS determined its entities' roles and responsibilities to meet its cybersecurity objectives, we analyzed relevant HHS documentation, such as organizational charts, for the full department, as well as for the Office of the Chief Information Officer (OCIO), Office of the Assistant Secretary for Preparedness and Response (ASPR), and Office of the National Coordinator for Health IT; departmental cybersecurity-related policies and procedures; strategic and operational plans; and HPH sector plans.

In reviewing these documents, we identified the HHS entities (e.g., offices, divisions, or centers) that had been assigned roles for managing cybersecurity within the department and for assisting with cybersecurity efforts in the HPH sector. We also reviewed HHS cybersecurity policies and procedures and strategic and operational plans, as well as HPH sector plans, to identify the responsibilities required to carry out the identified roles. We assessed the roles and responsibilities of the entities in comparison to the eight FISMA-defined elements of a cybersecurity program (discussed later in this report), and federal requirements related to cybersecurity in the HPH sector.

In addition, we used the steps recommended by GAO's fragmentation, overlap, and duplication evaluation guide to identify whether there was any fragmentation, overlap, or duplication in the responsibilities of the entities we identified with roles in cybersecurity.⁹ Specifically, we analyzed HHS documentation describing the entities' cybersecurity responsibilities to determine the:

- entities' goals and outcomes;
- entities' defined roles and responsibilities;
- relationships among the entities;

⁸GAO, *Standards for Internal Control in the Federal Government*, [GAO-14-704G](#) (Washington, D.C.: Sept. 10, 2014).

⁹GAO, *Fragmentation, Overlap, and Duplication: An Evaluation and Management Guide*, [GAO-15-49SP](#) (Washington, D.C.: Apr. 14, 2015).

-
- effects of any identified fragmentation, overlap, or duplication in the entities' roles and responsibilities; and
 - means by which the entities could increase efficiency and reduce or better manage the fragmentation, overlap, or duplication.

Further, we interviewed senior officials in HHS's OCIO, ASPR, and the Office of the National Coordinator for Health IT to verify that the HHS entities we identified had significant roles in managing the department's cybersecurity and in assisting the HPH sector with cybersecurity. We also discussed these officials' responsibilities for fulfilling those roles.

To address the third objective, we assessed control activities related to two key internal control principles that management should design control activities to achieve objectives and respond to risks, and implement control activities through the policies.¹⁰ Specifically, we assessed the department's efforts to use collaboration to manage its cybersecurity responsibilities by reviewing documentation of the management and operations of collaborative groups involved in addressing cybersecurity within the department and HPH sector.

To do this, we identified the groups that the HHS entities told us they used for cybersecurity collaboration within the department and HPH sector. We then selected for review, the seven cybersecurity-focused groups for which the HHS entities maintained operational documentation (i.e., charters and concepts of operation).¹¹ These collaborative groups were the

- HHS Chief Information Security Officer Council
- HHS Cloud Security Working Group
- HHS Continuous Monitoring and Risk Scoring Working Group

¹⁰[GAO-14-704G](#)

¹¹HHS officials in OCIO's Office of Information Security informed us that there are several working groups chartered under the Chief Information Security Officer Council. Those working groups include the Federal Information Security Modernization Act and the Cybersecurity Awareness, Training, and Education working groups. In addition, the six HHS operating divisions that we selected for this review informed us of other cybersecurity-related working groups, such as the HHS Incident Response Team, HHS IT Strategic Workforce, HHS Cybersecurity Workforce Development, Cyber Threat Coordination working groups, and others. However, the officials in the Office of Information Security did not provide charters or other documentation describing the operation of these working groups.

-
- Healthcare Threat Operations Center
 - HHS Cybersecurity Working Group
 - HPH Sector Government Coordinating Council's Cybersecurity Working Group
 - Joint HPH Cyber Working Group

We reviewed charters and concepts of operation for these collaborative groups to assess the management and operation of each group against seven leading collaboration practices that were identified in our prior work.¹² Those practices were:

- **Outcomes and accountability** address whether short- and long-term outcomes have been clearly defined, and the extent tracking and monitoring of progress in achieving outcomes has been performed.
- **Bridging organizational cultures** includes identifying the missions and cultures of the participating organizations in the collaborative groups.
- **Leadership** involves designating an individual who will lead the collaborative groups.
- **Clarity of roles and responsibilities** addresses whether the collaborative groups have clarified roles and responsibilities.
- **Participants** includes ensuring that all relevant participants are involved in the collaborative groups.
- **Resources** involves leveraging relevant staff and IT resources to support the operations of the collaborative groups.
- **Written guidance and agreements** includes documenting the collaborative groups' agreement regarding how they will collaborate and determining ways to continually update and monitor these agreements.

To further evaluate the effectiveness of the HHS entities' collaborative efforts as part of the third objective, we assessed the entities' information sharing processes as they pertain to three key principles of internal control information and communication activities: that management should use quality information to achieve the entity's objectives; internally

¹²GAO, *Results-Oriented Government: Practices That Can Help Enhance and Sustain Collaboration among Federal Agencies*, [GAO-06-15](#) (Washington, D.C.: Oct. 21, 2005) and *Managing for Results: Key Considerations for Implementing Interagency Collaborative Mechanisms*, [GAO-12-1022](#) (Washington, D.C.: Sept. 27, 2012).

communicate the necessary quality information to achieve the entity's objectives; and externally communicate the necessary quality information to achieve the entity's objectives.¹³ Specifically, we obtained documentation, such as flow charts and standard operating procedures, and interviewed senior officials to identify the processes used by the HHS entities to share cybersecurity information. We then compared the HHS entities' information sharing processes to the internal control standards that recommend management to identify relevant information from reliable sources to make informed decisions and address risks; communicate necessary quality information internally and externally; and use appropriate methods of communication for internal and external information sharing.

We supplemented our analyses by interviewing senior officials from the HHS OCIO, ASPR, and Office of the National Coordinator for Health IT. We obtained information on any challenges they had identified in collaborating with relevant sector partners to implement their roles and responsibilities for department and HPH sector cybersecurity.

Further, we interviewed officials charged with leading cybersecurity efforts in six HHS operating divisions. We obtained these officials' perspectives on the HHS entities' efforts to implement their roles and responsibilities for managing the department-wide cybersecurity program through its collaborative measures.

We selected the six operating divisions based on the number and type of information systems they operate (i.e., low-, moderate-, and high-impact),¹⁴ as reported in HHS's fiscal year 2019 FISMA report. The six operating divisions selected were the

- Food and Drug Administration

¹³[GAO-14-704G](#)

¹⁴Information systems are categorized according to the magnitude of harm or impact resulting from the system or its information being compromised. The *Standards for Security Categorization of Federal Information and Information Systems* define three impact levels where the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect (low), a serious adverse effect (moderate), or a severe or catastrophic adverse effect (high) on organizational operations, organizational assets, or individuals. *Federal Information Processing Standards Publication 199, Standards for Security Categorization of Federal Information and Information Systems* (Gaithersburg, Md.: February 2004).

-
- Centers for Medicare and Medicaid Services
 - Centers for Disease Control and Prevention (CDC)
 - Health Resource and Services Administration
 - Substance Abuse and Mental Health Services Administration
 - Agency for Health Research and Quality

We also interviewed the HPH Sector Coordinating Council’s Executive Director for Cybersecurity to obtain information on relevant HHS entities’ efforts to collaborate with private sector partners to implement their roles and responsibilities for HPH sector cybersecurity.¹⁵ Lastly, we interviewed senior officials at the Department of Homeland Security’s (DHS) Cybersecurity and Infrastructure Security Agency (CISA) to obtain information and documentation on their efforts to coordinate with HHS to share cybersecurity information and resources with the HPH sector. A more detailed description of our objectives, scope, and methodology can be found in appendix I.

We conducted this performance audit from November 2019 to June 2021 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.

Background

HHS’s mission is to enhance the health and well-being of Americans by providing for effective health and human services and fostering advances in the science underlying medicine, public health, and social services. The department is made up of several components that support the fulfillment of its mission. For example, the National Institutes of Health’s (NIH) mission is to seek knowledge about the nature and behavior of living systems and apply that knowledge to enhance health, lengthen life, and reduce illness and disability. Additionally, the CDC is responsible for leading national efforts to detect, respond to, and prevent illnesses and

¹⁵There are 16 critical infrastructure sectors that each have a sector coordinating council that consists of private organizations and functions as the principal entryway for the government to collaborate with each sector. Examples of private organizations in the HPH sector include medical facilities, health insurance companies, medical equipment and supply manufacturers, and pharmacies.

injuries that result from natural causes or the release of biological, chemical, or radiological agents.

Given HHS's knowledge and expertise in providing healthcare and improving public health, it serves as the lead federal agency responsible for coordinating security and resilience efforts for the HPH sector. The HPH sector provides services that are essential to maintaining local, national, and global health security. The organizations that make up the sector specifically include direct patient care facilities, health information technology vendors, health insurance companies, mass fatality management services, medical supply and equipment manufacturers, and laboratories and pharmacies.

HHS and the HPH Sector Have Been the Target of Malicious Cyber Activity

HPH sector organizations have been the targets for malicious cyber activity for the past 10 years. Most recently, COVID-19 has highlighted the need for HHS to pay continuous attention to cyber threats, which pose a serious challenge to national security, economic well-being, and public health and safety. Since the start of the nation's response to COVID-19 in March 2020, HHS and the HPH sector organizations have been targets for malicious cyber activity.

The following examples of incidents and alerts illustrate how the actions by malicious actors have targeted patient information, intellectual property, public health data, and intelligence. Specifically,

- In March 2020, HHS was the target of a distributed denial-of-service cyberattack.¹⁶ The former Secretary of HHS reported that no data were breached and the agency's operations were not impacted. Nevertheless, during a May 2020 meeting with officials from the department's OCIO, the former Chief Information Officer informed us that HHS had been targeted daily with sophisticated cyberattacks since March 15, 2020.
- In May 2020, CISA released a joint alert with the United Kingdom's National Cyber Security Centre regarding advanced persistent threat groups exploiting COVID-19 to target healthcare and essential

¹⁶A distributed denial-of-service attack uses traffic generated from many different sources to create a high-volume of traffic directed toward an intended target, resulting in disruptions and damages.

services.¹⁷ The alert warned that advanced persistent threat groups were frequently targeting organizations in order to collect bulk personal information, intellectual property, and intelligence that aligns with national priorities.

- In May 2020, CISA and the Federal Bureau of Investigation (FBI) issued a joint public service announcement to raise awareness of a threat to COVID-19-related research.¹⁸ The announcement stated that cyber actors associated with the People's Republic of China had been observed attempting to identify and obtain valuable intellectual property and public health data related to vaccines, treatments, and testing from networks and personnel affiliated with COVID-19-related research. As a result, the FBI and CISA urged organizations conducting research in these areas to maintain cybersecurity practices to prevent surreptitious review or theft of COVID-19-related material.
- In October 2020, CISA, the FBI, and HHS issued a joint cybersecurity advisory alert¹⁹ regarding ransomware activity targeting the HPH sector.²⁰ The alert described tactics, techniques, and procedures used by cybercriminals to infect systems operated in the sector with ransomware for financial gain. CISA, FBI, and HHS suggested several actions to mitigate the threat, including that the HPH sector organizations review or establish patching plans, security policies, user agreements, and business continuity plans to ensure they address current threats posed by malicious cyber actors.

¹⁷CISA and United Kingdom National Cyber Security Centre, *APT Groups Target Healthcare and Essential Services* (Washington, D.C.: May 5, 2020). The *Cybersecurity and Infrastructure Security Agency (CISA) Act of 2018* established CISA as an operational component agency within the Department of Homeland Security, and assigned CISA the responsibility to advance the mission of protecting federal civilian agencies' networks from cyber threats and to enhance the security of the nation's critical infrastructures in the face of both physical and cyber threats. *Cybersecurity and Infrastructure Security Agency Act of 2018*, Pub. L. No. 115-278, 132 Stat. 4168, 4169, section 2 (Nov. 16, 2018) (codified at 6 U.S.C. § 652).

¹⁸FBI and CISA, *People's Republic of China (PRC) Targeting of COVID-19 Research Organizations* (Washington, D.C.: May 13, 2020).

¹⁹CISA, FBI, and HHS, *Joint Cybersecurity Advisory: Ransomware Activity Targeting the Healthcare and Public Health Sector* (Washington, D.C.: October 28, 2020).

²⁰According to DHS, ransomware is a type of malicious software cyber actors use to deny access to systems or data. The malicious cyber actor holds systems or data hostage until the ransom is paid. After the initial infection, the ransomware attempts to spread to shared storage drives and other accessible systems. If the demands are not met, the system or encrypted data remain unavailable, or data may be deleted.

Any disruption in the systems used by HHS and the HPH sector organizations could be catastrophic for the many Americans who rely on their services. For example, a cyberattack resulting in the disruption of IT systems supporting pharmacies, hospitals, and physicians' offices would interfere with the approval and distribution of the life-saving medications and other products needed by patients and healthcare facilities. Without proper safeguards, computer systems are vulnerable to individuals and groups with malicious intent who can intrude and use their access to obtain sensitive information, commit fraud and identity theft, disrupt operations, or launch attacks against other computer systems and networks.

Federal Laws and Guidance Set Requirements for HHS to Address Cybersecurity within the Department and the HPH Sector

Given the importance of protecting federal agencies' systems and information, Congress has enacted laws and the National Institute of Standards and Technology (NIST) has issued guidance applicable to agencies in managing and protecting their cyber assets. Specifically, FISMA established requirements for federal agencies, including HHS, to address cybersecurity within their operating environment. The act provides a comprehensive framework for ensuring effective controls over information resources that support federal operations and assets, among other things.

The act requires agencies to develop and implement an agency-wide cybersecurity program that includes the following eight elements:

1. periodic risk assessments;
2. cost-effective policies and procedures that address cybersecurity throughout the life cycle of information systems and ensure compliance with federal guidelines and standards;
3. subordinate plans for providing cybersecurity protections on networks, facilities, and systems;
4. security awareness training for personnel, including contractors;
5. periodic testing and evaluation of the effectiveness of cybersecurity policies, procedures, and practices;
6. a process for managing remedial actions to address deficiencies in cybersecurity policies, procedures, and practices;
7. procedures for detecting, reporting, and responding to security incidents; and
8. plans and procedures to ensure continuity of operations for information systems.

The law also requires that the inspector general or independent external auditor for each agency, including HHS, perform an annual independent evaluation to determine the effectiveness of the cybersecurity policies, procedures, and practices supporting the agency's cybersecurity program.

NIST Special Publication 800-53, revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, directs agencies to develop and disseminate an agency-wide cybersecurity program plan for implementing FISMA.²¹ According to this publication, the plan should:

- provide an overview of the program's requirements and a description of the security controls in place or planned for meeting those requirements;
- identify and assign roles and responsibilities for implementing the plan;
- reflect the coordination among organizational entities responsible for information security; and
- be approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations, assets, individuals, other organizations, and the nation.

In addition, requirements set in federal laws and policies direct federal agencies with leading roles in critical infrastructure security, such as HHS, to assist critical infrastructure sectors with improving their cybersecurity. Specifically:

- PPD 21, *Critical Infrastructure Security and Resilience*. PPD 21 identified the HPH sector as one of 16 critical infrastructure sectors and designated HHS as its sector-specific agency, or sector risk

²¹National Institute of Standards and Technology, *Security, and Privacy Controls for Federal Information Systems and Organizations*. Special Publication 800-53, revision 4 (Gaithersburg, M.D.: April 2013). The institute updated this publication in September 2020 with the issuance of revision 5. See NIST, *Security and Privacy Controls for Information Systems and Organizations*. Special Publication 800-53, revision 5 (Gaithersburg, M.D.: September 2020). Agencies will be required to adhere to the updated publication by September 2021, at which time revision 4 will be withdrawn.

management agency.²² As defined in PPD 21, the roles and responsibilities of the sector risk management agency include:

- collaborating with critical infrastructure owners and operators; independent regulatory agencies, where appropriate; and with state, local, tribal, and territorial entities, as appropriate;
- serving as a day-to-day federal interface for the prioritization and coordination of sector-specific activities;
- carrying out incident management responsibilities consistent with statutory authority and other appropriate policies, directives, or regulations; and
- providing, supporting, or facilitating technical assistance and consultations for their respective sector to identify vulnerabilities and help mitigate incidents, as appropriate.

According to the directive, implementation of these roles and responsibilities should consider all hazards, including cybersecurity threats, and are intended to identify and disrupt threats and hasten response and recovery, among other things.

- Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*. The executive order was issued in February 2013 to enhance the security and resilience of the nation’s critical infrastructure and maintain a cyber environment that promotes safety, security, and privacy.²³ It called for the sector risk management agency to, among other things,
 - work in coordination with the Department of Homeland Security to establish a voluntary program to support the adoption of the *NIST Framework for Improving Critical Infrastructure Cybersecurity* by owners and operators of critical infrastructure and any other interested entities;

²²During the course of our audit, evidentiary documentation provided by the agencies refers to PPD 21 and sector-specific agencies. However, the William M. (Mac) Thornberry *National Defense Authorization Act for Fiscal Year 2021* (NDAA) states that the term “sector risk management agency” replaces the term “sector-specific agency” in the *Homeland Security Act of 2002*. The NDAA amends the *Homeland Security Act of 2002* and sets out sector risk management agency responsibilities within this critical infrastructure framework. Pub. L. No. 116-283, § 9002, 134 Stat. 3388, 4768 (Jan. 1, 2021).

²³The White House, Executive Order No. 13636, 78 Fed. Reg. 11,739 (Feb. 19, 2013).

-
- create incentives to encourage owners and operators of critical infrastructure to participate in the voluntary program; and
 - if necessary, develop implementation guidance or supplemental materials to address sector-specific risks and operating environments.²⁴
 - *Cybersecurity Act of 2015*. The act includes requirements for HHS to improve cybersecurity in the healthcare industry by, for example, establishing a common set of voluntary and industry-led guidelines, best practices, and procedures that cost-effectively reduce cybersecurity risks at healthcare organizations and improve safeguards to address cybersecurity threats.²⁵ According to the act, these guidelines, best practices, and procedures should be consistent with NIST guidelines and standards, as well as with the *Health Insurance Portability and Accountability Act of 1996* (HIPAA) privacy and security regulations. Lastly, these documents are to be established in collaboration with DHS, NIST, healthcare industry stakeholders, and other relevant federal and industry entities.²⁶
 - *Health Information Technology for Economic and Clinical Health Act* (HITECH Act). The HITECH Act established the Office of the National Coordinator for Health IT to support the development of a nationwide health IT infrastructure that facilitates the electronic use and exchange

²⁴The National Institute of Standards and Technology developed the *Framework for Improving Critical Infrastructure Cybersecurity* (cybersecurity framework) to provide a set of industry standards and best practices to help the owners and operators of critical infrastructure with managing cybersecurity risks. The National Institute of Standards and Technology released the first iteration of the draft on February 12, 2014, and released an update to the framework on April 16, 2018. National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, version 1.1 (Gaithersburg, Md.: Apr. 16, 2018).

²⁵The *Cybersecurity Act of 2015* was enacted as part of the *Consolidated Appropriations Act, 2016*, Pub. L. No. 114-113, div. N, § 405, 129 Stat. 2242, 2981 (Dec. 18, 2015).

²⁶HHS convened the *Cybersecurity Act of 2015* 405(d) Task Group and developed the *Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients*. It details 10 cybersecurity practices related to email and endpoint protection systems; access management; data protection and loss prevention; asset, network, and vulnerability management; incident response; medical device security, and cybersecurity policies.

of information.²⁷ The act states that, among other things, the health IT infrastructure should ensure that patient health information is secure and protected in accordance with applicable law. The act directs the Office of the National Coordinator for Health IT to coordinate HHS's health IT policies and programs with those of other relevant federal agencies to avoid duplication. According to the act, this coordination is also intended to help ensure that agencies undertake health IT activities primarily within the areas that they have greatest expertise and technical capability.

- *Health Insurance Portability and Accountability Act of 1996 (HIPAA)*. HIPAA authorized the Secretary of HHS to establish standards to protect the privacy of certain health information and requires the Secretary to adopt security standards for that information.²⁸ HHS promulgated regulations implementing the act's provisions through its issuance of the HIPAA Rules—Privacy, Security, and Enforcement.²⁹ The HIPAA Rules, as amended by the HITECH Act, govern protected health information transmitted or maintained by covered entities and their business associates.³⁰ Specifically,
 - The Privacy Rule generally prohibits the use and disclosure of protected health information except in the circumstances set out in the regulations.
 - The Security Rule established national standards intended to safeguard individuals' electronic protected health information that is created, received, used, or maintained by a covered entity.³¹ The rule requires appropriate administrative, physical, and

²⁷The HITECH Act was enacted as Title XIII of Division A and Title IV of Division B of the *American Recovery and Reinvestment Act*, Pub. L. No. 111-5, Title XIII, 123 Stat. 115, 226 (Feb. 17, 2009). It defines health IT as hardware, software, integrated technologies or related licenses, intellectual property, upgrades, or packed solutions sold as services that are designed for, or support, the use by health care entities or patients for the electronic creation, maintenance, access, or exchange of health information.

²⁸Pub. L. No. 104-191, Title II, Subtitle F, 110 Stat. 1936, 2021 (Aug. 21, 1996).

²⁹The *HIPAA Privacy, Security, and Enforcement Rules* were promulgated at 45 C.F.R. Parts 160 and 164.

³⁰Entities covered by HIPAA include health plans, health care providers, and health care clearinghouses. Business associates of these entities create, receive, maintain, or transmit patient protected health information on behalf of a covered entity. 45 C.F.R. § 160.103.

³¹45 C.F.R. Part 164, Subpart C, §§ 164.302-318.

technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.

- The Enforcement Rule established the department's processes to ensure compliance with the HIPAA Rules by a covered entity. It contains provisions relating to HHS investigations, rules governing civil monetary penalties against covered entities or business associates deemed by the Secretary of HHS to be in violation of a HIPAA provision, and rules governing the procedures for hearings and appeals where a covered entity challenges a violation determination.³²
- CARES Act. Enacted in March 2020, the act requires HHS to issue guidance about sharing patient protected health information during the COVID-19 public health and national emergency.³³ The guidance is required to include information on complying with HIPAA regulations and any policies that become effective during such an emergency.

In accordance with the federal requirements listed, three main HHS offices are responsible for implementing protections to secure their own systems and for providing assistance and guidance on cybersecurity to the department's components and the organizations in the HPH sector.

- The HHS OCIO is responsible for leading the development and implementation of an enterprise IT infrastructure across HHS and its component agencies. In doing so, the office is to establish and provide support for various IT initiatives, to include cybersecurity. The HHS OCIO's Office of Information Security leads its cybersecurity efforts.
- ASPR is responsible for leading collaboration and coordination efforts to strengthen the security and resilience of the HPH sector. ASPR's Critical Infrastructure Protection Division, with the support of entities in the OCIO's Office of Information Security, is tasked with managing the collaboration and coordination efforts for cybersecurity, as discussed later in this report.
- The Office of the National Coordinator for Health IT, working with the HHS Office for Civil Rights and other federal agencies, is responsible for coordinating the implementation of a nationwide health information

³²45 C.F.R. Part 160, Subparts C, D, and E.

³³The CARES Act provided over \$2 trillion in emergency assistance and health care response for individuals, families, and businesses affected by COVID-19. Pub. L. No. 116-136, § 3224, 134 Stat. 281, 380 (March 27, 2020).

exchange that allows the secure use and transmission of patient health information.

HHS Has Clearly Defined Roles and Responsibilities for Managing the Cybersecurity of the Department

According to GAO's Fragmentation, Overlap, and Duplication Evaluation Guide, organizations can avoid providing fragmented, overlapping, and duplicative services and activities by clearly and distinctly defining the roles and responsibilities for those organizations.³⁴ Doing so would also reduce the risk of those organizations being wasteful and inefficient.

With regard to cybersecurity, FISMA requires federal agencies to develop, document, and implement a cybersecurity program.³⁵ NIST guidance states that an effective cybersecurity program should be based, in part, on the implementation of a program plan that identifies and assigns roles and responsibilities for implementing the plan.³⁶ The plan should explain what roles and responsibilities an agency has assigned to address the eight elements of a cybersecurity program, as defined by FISMA.

HHS clearly described roles and responsibilities for implementing its cybersecurity program, including the eight elements of the program required by FISMA, in two official department documents. The *HHS Information Systems Security and Privacy Policy* designates the role of managing cybersecurity for the department to the HHS Chief Information Security Officer (CISO), who leads the HHS OCIO's Office of Information Security.³⁷ The *Office of Information Security Services Catalog* describes the responsibilities of the office in supporting the CISO's management of the department's cybersecurity program.³⁸

The Office of Information Security is made up of six divisions, each tasked with fulfilling the responsibilities identified in the services catalog. Three of the six divisions had been assigned clear responsibilities that

³⁴[GAO-15-49SP](#)

³⁵Pub. L. No. 113-283, 128 Stat. 3073, 3079, § 2 (Dec. 18, 2014), amended 44 U.S.C. § 3554.

³⁶NIST, *Security, and Privacy Controls for Information Systems and Organizations*. NIST Special Publication 800-53, revision 5 (Gaithersburg, M.D.: Sept. 2020).

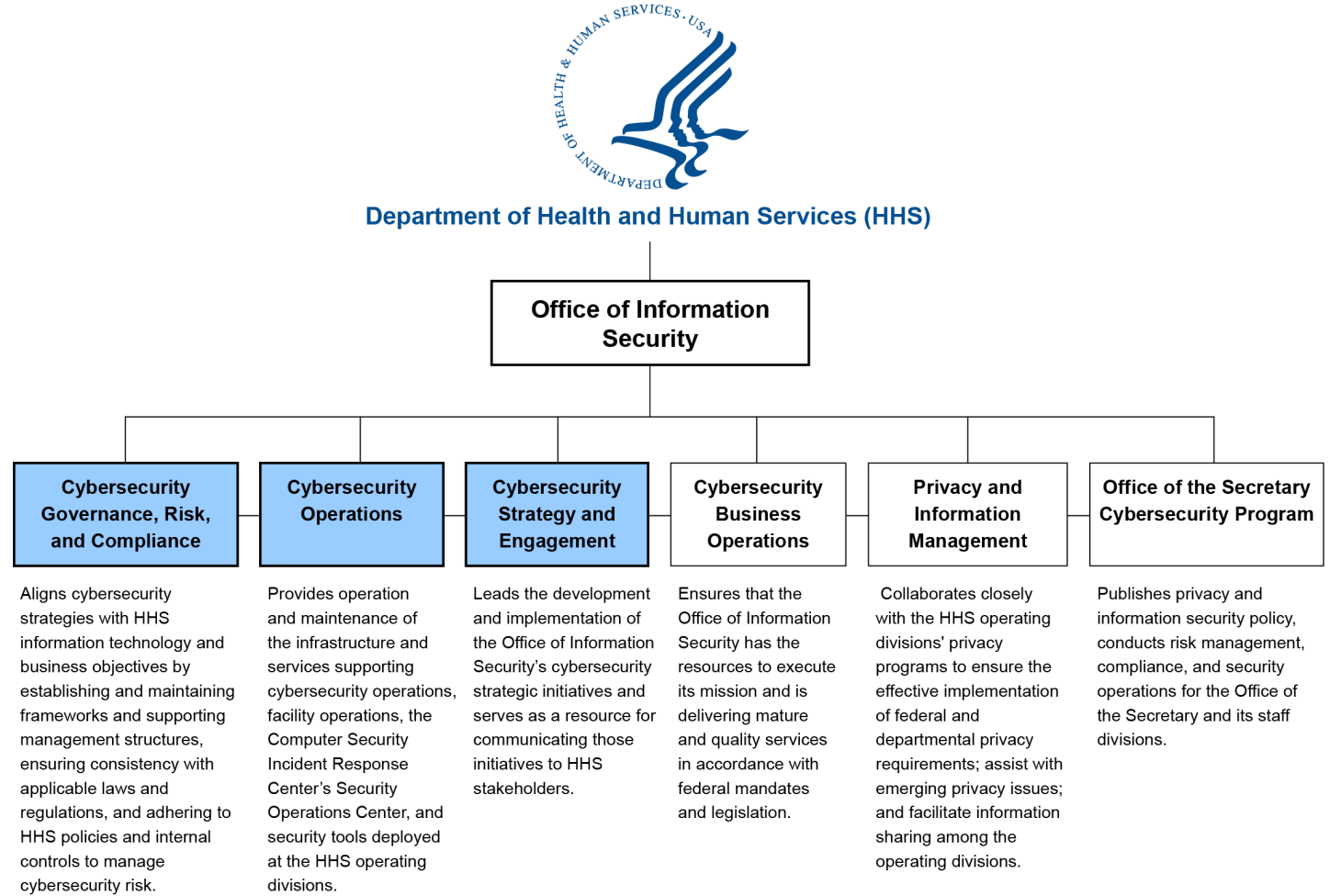
³⁷Department of Health and Human Services, *HHS Information Systems Security and Privacy Policy*, (Washington, D.C.: July 30, 2014).

³⁸Department of Health and Human Services, *Office of Information Security Services Catalog, Version 1.4* (Washington, D.C.: June 2020).

directly support the department's implementation of the eight FISMA-defined elements of a cybersecurity program. As shown in figure 1, these divisions are:

- Cybersecurity Governance, Risk, and Compliance
- Cybersecurity Operations
- Cybersecurity Strategy and Engagement

Figure 1: Structure of the Department of Health and Human Services (HHS) Office of the Chief Information Officer’s Office of Information Security



The three Office of Information Security divisions that have responsibilities for implementing the eight elements of a cybersecurity program, as defined by the *Federal Information Security Modernization Act of 2014*

Source: GAO analysis of Department of Health and Human Services documentation. | GAO-21-403

The OCIO Office of Information Security clearly defined responsibilities for the three divisions that address the eight elements of a cybersecurity program, as outlined in FISMA. Specifically:

- The Cybersecurity Governance, Risk, and Compliance Division is responsible for six of the eight cybersecurity program elements—

performing periodic risk assessments; developing cybersecurity policies and procedures; maintaining subordinate plans; providing security training; implementing information security continuous monitoring; and managing a remedial action process.

- The Cybersecurity Operations division is responsible for one of the cybersecurity program elements—implementing an incident response process.
- The Cybersecurity Strategy and Engagement Division had responsibilities related to three of the eight cybersecurity program elements—maintaining subordinate plans; implementing information security continuous monitoring; and managing a remedial action process.

Table 1 lists the FISMA-defined elements and a description of the responsibilities that HHS had assigned to the three Office of Information Security divisions to address each element.

Table 1: Responsibilities for the Three Office of Information Security Divisions Managing the Department of Health and Human Services' (HHS) Cybersecurity Program, in accordance with *Federal Information Security Modernization Act of 2014 (FISMA)*

FISMA-defined element for a cybersecurity program	HHS responsibility for addressing the FISMA-defined element
Periodic risk assessments	<p>The Cybersecurity Governance, Risk, and Compliance Division is responsible for:</p> <ul style="list-style-type: none"> • Managing the department's cybersecurity risk management program, which involves continually providing situational awareness of HHS's risk posture by identifying, assessing, remediating, and monitoring security risks. • Providing management and oversight of the department's implementation of the government-wide high-value asset program, which requires agencies to identify and prioritize their high-value assets^a and perform risk assessments on those assets at least once every three years.
Cybersecurity policies and procedures	<p>The Cybersecurity Governance, Risk, and Compliance Division is responsible for:</p> <ul style="list-style-type: none"> • Developing all cybersecurity policies and procedures that are intended to provide the baseline security requirements that the HHS operating and staff divisions are required to implement. • Managing the entire life cycle of the policies it develops, including creating new policies, updating existing ones, and maintaining them until no longer applicable.
Subordinate plans	<ul style="list-style-type: none"> • The Cybersecurity Strategy and Engagement Division is responsible for ensuring that system-level security documentation, such as system security plans, are maintained for systems throughout the department. • The Cybersecurity Governance, Risk, and Compliance Division is responsible for reviewing the system security plans of the cloud services and products authorized through the Federal Risk and Authorization Management Program (FedRAMP).^b

FISMA-defined element for a cybersecurity program**HHS responsibility for addressing the FISMA-defined element**

Security training

The Cybersecurity Governance, Risk, and Compliance Division is responsible for:

- Developing the curriculum for annual cybersecurity awareness training required for all employees and contractors with access to HHS networks, applications, or data.
- Developing a training curriculum for role-based training that is commensurate with the roles and responsibilities of HHS staff with significant responsibility for cybersecurity.
- Tracking staff progression in taking both cybersecurity awareness and role-based training.^c
- Providing training and presentations on cloud security and the FedRAMP process, which includes training and education with stakeholders to inform and educate audiences on the HHS FedRAMP program's policies, processes, and procedures.

Information security continuous monitoring

- The Chief Information Security Officer is responsible for coordinating the department's continuous monitoring efforts to ensure the programs implemented by each operating and staff division complies with the HHS Information Security Continuous Monitoring Strategy.

The Cybersecurity Strategy and Engagement Division is responsible for:

- Providing continuous monitoring process support by ensuring that system audit logs are reviewed, security documentation and inventories are updated, and security controls are assessed.
- Performing technical vulnerability analyses to validate systems' readiness for authority to operate.
- Validating security control assessments performed on systems throughout HHS.

The Cybersecurity Governance, Risk, and Compliance Division is responsible for:

- Reviewing security documentation supporting ongoing assessment and authorization of the department's cloud services and products approved through FedRAMP.
- Conducting high-value asset evaluations, which involve utilizing DHS requirements and NIST guidance to perform ongoing authorization of the department's high-value assets.^d
- Serving as the department's liaison to the HHS Office of the Inspector General for its annual FISMA-required evaluation to determine the effectiveness of the department's cybersecurity. More specifically, the division is responsible for managing the Inspector General's evaluation at the department level and within the selected operating divisions.

Remedial action process

The Cybersecurity Strategy and Engagement Division is responsible for:

- Developing, managing, and reporting on the resulting remediation efforts for the security control assessments it supports throughout the department.

The Cybersecurity Governance, Risk, and Compliance Division is responsible for:

- Tracking the status of remedial actions resulting from security control assessments performed on the department's cloud products and services authorized through FedRAMP.
 - Providing DHS with remediation plans that address findings from the DHS-led high-value asset assessments.
 - Maintaining records on the status of all audit recommendations and remedial efforts throughout HHS and its operating divisions, to include those resulting from the Office of the Inspector General's FISMA evaluation of HHS and the cybersecurity reviews GAO performs at the department.
-

FISMA-defined element for a cybersecurity program**HHS responsibility for addressing the FISMA-defined element**

Incident response process

The Cyber Security Operations Division's Computer Security Incident Response Center is responsible for:

- Managing the department's incident response process.
 - Serving as the primary point of contact for incident notification and reporting to the department's operating and staff divisions and DHS.
 - Maintaining partnership with the computer security incident response teams throughout HHS to ensure awareness of security vulnerabilities, threats, and incidents that may negatively impact the department's fulfillment of its many missions and functions.
-

Contingency plans and procedures

The HHS Chief Information Security Officer is responsible for ensuring that controls supporting contingency plan development, contingency plan testing, and information system backup, among others, are implemented at the department's staff and operating divisions. The operating and staff divisions are responsible for implementing their systems' contingency plan controls.

Source: The Department of Health and Human Services' Information Systems Security and Privacy Policy and Office of Information Security Services Catalog, version 1.4 | GAO-21-403

^aA high value asset is a designation for federal information or a federal information system that (1) is of high value to the federal government or its adversaries; (2) is necessary for the owning agency to accomplish its primary mission essential functions, as approved in accordance with Presidential Policy Directive 40 on the *National Continuity Policy*, within expected timelines; or (3) serves a critical function in maintaining the security and resilience of the federal civilian enterprise. Office of Management and Budget, *Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program*, M-19-03 (Washington, D.C.: Dec. 10, 2018).

^bThe Office of Management and Budget established FedRAMP in 2011 with the intent to provide a standardized approach for selecting and authorizing the use of cloud services that meet federal security requirements.

^cAccording to a June 2017 memo regarding requirements for role-based training of personnel with significant security responsibilities, each HHS operating division's Chief Information Security Officer is responsible for tracking and maintaining the training records for all employees and contractors they identified as with significant security responsibilities, in coordination with the operating divisions Training Coordinators and Contracting Officers/Representatives.

^dThe *HHS Policy for the High-Value Asset Program* states that the high-value asset program management office is currently working towards aligning evaluation capabilities with DHS requirements. The policy states that, once the program management office determines that it is able to meet requirements set forth by DHS, the HHS high-value asset evaluation methodology will be updated accordingly and evaluations will then be offered to the HHS operating and staff divisions.

Although the Office of Information Security's Cybersecurity Governance, Risk, and Compliance Division and Cybersecurity Strategy and Engagement Division both have responsibilities related to subordinate plans, information security continuous monitoring, and remedial actions, the defined responsibilities have been clearly separated. Specifically, as the main division with a role in ensuring the department's consistency with cybersecurity laws and regulations, the Cybersecurity Governance, Risk, and Compliance Division's responsibilities for subordinate plans, information security continuous monitoring, and remedial actions are specific to HHS's implementation of federal requirements for cloud services and products and high-value assets. With its role in serving as a resource for the department's cybersecurity initiatives, the Cybersecurity

Strategy and Engagement’s responsibilities include all other systems maintained throughout the department.

HHS Clearly Defined Its Roles and Responsibilities for Supporting HPH Sector Cybersecurity; However, Opportunity for Improving Coordination Exists

HHS developed, or contributed to the development of, policies, procedures, and plans that described the department’s roles and responsibilities for providing cybersecurity support to the HPH sector. However, the procedures and plans did not describe coordination among two entities that are critical to the department’s cybersecurity information sharing with the HPH sector—the Health Sector Cybersecurity Coordination Center (HC3) and the Healthcare Threat Operations Center (HTOC). Without coordinating the responsibilities for sharing cybersecurity information to the HPH sector, HHS is missing an opportunity to strengthen those efforts for their intended audience.

HHS Designated Roles and Defined Responsibilities for Entities Supporting Cybersecurity in the HPH Sector

PPD 21 and the *Cybersecurity Act of 2015* require HHS to coordinate cybersecurity efforts in the HPH sector. In addition, the HITECH Act and HIPAA direct the department to ensure the protection of certain health information that is processed and transmitted throughout the sector.³⁹ Further, NIST guidance suggests activities and outcomes that agencies can implement to manage cybersecurity risks to critical infrastructure. Specifically, the NIST *Framework for Improving Critical Infrastructure Cybersecurity* states that agencies should establish roles and responsibilities that enable them to achieve their objectives.⁴⁰

As the designated sector risk management agency for the HPH sector, and in accordance with federal guidance, HHS assigned responsibilities for coordinating cybersecurity resilience efforts to several of its entities. Specifically, HHS policies, procedures, and plans described the responsibilities of four of the department’s entities to fulfill its sector risk management agency role. These entities are the

- Office of the Assistant Secretary for Preparedness and Response (ASPR);
- Office of Information Security;

³⁹The HIPAA regulations, as amended by the HITECH Act, govern protected health information held or transmitted by covered entities and their business associates.

⁴⁰NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, version 1.1 (Gaithersburg, Md.: Apr. 16, 2018).

-
- HC3; and
 - HTOC.

In addition, HHS assigned responsibilities to one entity to fulfill its national health IT coordinator role, in accordance with federal criteria. In this regard, the HHS Office of the National Coordinator for Health IT is the entity designated to facilitate a nationwide health IT infrastructure. As such, the office is responsible for ensuring that the health IT infrastructure allows the secure use and exchange of health information and has defined responsibilities for fulfilling that role.⁴¹

Table 2 describes the role for each HHS entity that supports the department's cybersecurity assistance to the HPH sector and the responsibilities for fulfilling those roles.

⁴¹Pub. L. No. 111-5, § 13101, 123 Stat. 230 (Feb. 17, 2009), 83 Fed. Reg. 19289 (May 02, 2018).

Table 2: Roles and Responsibilities of the Department of Health and Human Services (HHS) Entities that Provide Cybersecurity Assistance to the Healthcare and Public Health (HPH) Critical Infrastructure Sector

HHS entity	Description of the role	Description of the responsibilities
Office of the Assistant Secretary for Preparedness and Response (ASPR)	ASPR's Critical Infrastructure Protection Division is to fulfill HHS's role as the sector risk management agency for the HPH sector. The division is to promote resilience in the sector to manage risk and coordinate an effective response to new cybersecurity threats.	<ul style="list-style-type: none"> • Leading the HPH government coordinating council, which provides effective coordination of sector risk management strategies and activities, policies, and communication across government agencies and between the government and the private sector. For cybersecurity, the division is to lead the Government Coordinating Council's Cybersecurity Working Group; and co-lead the Joint HPH Cybersecurity Working Group, along with industry partners. • Coordinating the development of cybersecurity incident response plans and exercises intended to prepare the HPH sector for potential incidents. The division also works with the HPH sector's industry partners during incident response and recovery operations to gain an understanding of the impacts certain incidents could have on the sector. ASPR is to use that understanding to inform incident restoration and recovery planning, and operational activities. Additionally, ASPR provides advice and counsel throughout a cyber threat and incident and maintains ongoing coordination with the HC3 and the Department of Homeland Security. • Assessing gaps and challenges in the current operating environment of the HPH sector and providing risk mitigation recommendations for physical and cyber-related supply chains. According to senior officials at ASPR and HC3, ASPR relies on HC3 as the subject matter expert for cybersecurity to assist with providing cybersecurity technical assistance to the HPH sector. ASPR officials also stated that they rely on the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency and the Federal Bureau of Investigation for their subject matter expertise in cybersecurity.
Office of Information Security	The Office of Information Security's Cybersecurity Governance, Risk, and Compliance Division supports the department's role as sector risk management agency by coordinating efforts to improve the cybersecurity of the sector with public and private industry partners. The division is to manage and implement the requirements of Section 405(d) of the <i>Cybersecurity Act of 2015</i> , which directs HHS to improve cybersecurity in the healthcare industry by taking actions towards aligning healthcare industry security approaches. ^a	<p>The Office of Information Security's Cybersecurity Governance, Risk, and Compliance Division, through its Section 405(d) activities, is responsible for:</p> <ul style="list-style-type: none"> • Engaging with public and private sector stakeholders to develop and distribute cybersecurity resources for use across the HPH sector. • Facilitating and supporting public-private sector collaborations through working groups and task groups.

HHS entity	Description of the role	Description of the responsibilities
Health Sector Cybersecurity Coordination Center (HC3)	HC3, formerly known as the Health Cybersecurity and Communications Integration Center, is a branch of the Office of Information Security's Cybersecurity Operations Division. It was established to improve cybersecurity information sharing between HHS, its federal partners, and the HPH sector. HC3 is expected to collaborate with the HPH sector to understand persistent cyber threats, learn adversaries' patterns and trends, and provide information and approaches on how the sector can better defend itself.	<ul style="list-style-type: none"> Facilitating cybersecurity information sharing between organizations in the HPH sector and managing and supporting cybersecurity information sharing platforms that facilitate partnerships. This includes the dissemination of HC3-branded products that provide cybersecurity best practices, relevant and actionable cyber threat and vulnerability intelligence, and mitigation techniques and strategies. Collecting and analyzing threat indicators and known system vulnerabilities affecting the HPH sector, and tracking cyber campaigns and techniques affecting the sector. Supporting the development of cybersecurity exercises and training for the HPH sector.
Healthcare Threat Operations Center (HTOC)	HTOC is an interagency program supported by analysts from HHS and its federal healthcare partners, the Department of Veterans Affairs, and the Defense Health Agency. It operates under the Office of Information Security's Cybersecurity Operations Division and serves as a centralized federal healthcare threat operations center. HTOC is expected to leverage cyber threat data to improve the information security posture of the healthcare infrastructure of the federal healthcare partners and provide the ability to deter, detect, and remove cyber threats.	<ul style="list-style-type: none"> Providing timely, accurate, descriptive, and actionable cybersecurity data. Developing and disseminating cyber alerts, cyber warnings, and threat intelligence information. Supporting the early detection and remediation of incidents for the federal healthcare partners.
Office of the National Coordinator for Health Information Technology (ONC)	<p>ONC consists of four offices that support its role as coordinator for facilitating development of a health IT infrastructure to support the electronic use and exchange of health information:</p> <ul style="list-style-type: none"> The Immediate Office of the National Coordinator is to provide decision-making and strategic direction for executing ONC's mission and implementing its functions. The Office of Policy is to manage ONC's policy development and rulemaking activities. The Office of Technology is to provide support for the technological aspects of facilitating development of a health IT infrastructure that allows the electronic use and exchange of health information. The Office of the Chief Operating Officer is to provide administrative services to ONC, such as executive secretarial and financial and budget management support. 	<ul style="list-style-type: none"> The ONC Chief Privacy Officer is responsible for advising the National Coordinator for Health Information Technology on the security of electronic health information and coordinating with federal, state, regional, and foreign entities on the security of electronic individually identifiable health information. The ONC Office of Policy is responsible for conducting advanced analysis and evaluation of HHS and ONC policies for health information technology security. ONC, working with the HHS Office for Civil Rights and other federal agencies, is responsible for coordinating the implementation of the nationwide health information technology exchange that considers information security practices, in accordance with the <i>Health Insurance Portability and Accountability Act of 1996</i>.^b

Source: *Healthcare and Public Health Sector-Specific Plan* (Washington, D.C.: May 2016); HHS, *ASPR Strategic Plan for 2020-2023* (Washington, D.C., April 2020); HHS, *Assistant Secretary for Preparedness and Response Incident Response Framework*, version 2.1 (Washington D.C., April 3, 2019); HHS, *Office of Information Security Services Catalog*, version 1.4 (Washington, D.C.: June 2020); HHS, *Office of Information Security Cybersecurity Operations Operational Plan*, version 1.0 (Washington, D.C., October 2019); HHS, *Health Sector Cybersecurity Coordination Center Strategic Plan 2018-2020* (Washington, D.C.: Jan. 2019); *Healthcare Threat Operations Center Concept of Operations* (Washington, D.C.; April 2020); and 83 Federal Register. 19289 (May 02, 2018). | GAO-21-403.

^aThe *Cybersecurity Act of 2015* was enacted as part of the *Consolidated Appropriations Act, 2016*, Pub. L. No. 114-113, div. N, § 405, 129 Stat. 2242, 2981 (Dec. 18, 2015).

^bThe HHS Office for Civil Rights is responsible for enforcing the *Health Insurance Portability and Accountability Act of 1996* security regulations that protect the security of patients' health information, among other things.

Two HHS Entities Are Not Coordinating with Each Other to Fulfill Their Information Sharing Responsibilities

As mentioned earlier in this report, organizations can avoid fragmented, overlapping, and duplicative services and activities by clearly and distinctly defining the roles and responsibilities within those organizations.⁴² In addition, organizations with responsibilities in the same broad area of service delivery can strengthen implementation of those responsibilities through coordination.

HHS clearly defined the responsibilities for HC3 and HTOC in the HC3 Strategic Plan and HTOC Concept of Operations. Specifically, HC3 was established to improve cybersecurity information sharing among HHS, its federal partners, and the HPH sector. To this end, the HC3 Strategic Plan states that HC3 is responsible for ensuring that the HPH sector has the latest threat information, engages in routine and coordinated risk information sharing, protects against advanced persistent threats, and develops proactive risk management strategies.

In addition, HTOC was established to provide the federal healthcare partners—HHS, the Department of Veterans Affairs, and the Defense Health Agency—with situational awareness that strengthens the security and resilience of the federal healthcare IT systems, networks, and critical infrastructure. The HTOC Concept of Operations states that HTOC is to support efforts to strengthen cybersecurity collaboration and coordination activities across the HPH sector by improving the information security posture of the healthcare ecosystem and the collective ability to deter, detect, and remove cyber threats.

However, HC3 does not receive actionable cyber threat information from HTOC, and thus is unable to provide the HPH sector with information to potentially strengthen cyber response and protection efforts. Based on the alerts and reports we reviewed, HC3's alerts included mitigation strategies that healthcare organizations could implement to mitigate threats. In addition, the HTOC reports included actionable cyber threat information, such as the Internet Protocol address that was used by a

⁴²[GAO-15-49SP](#)

malicious actor to facilitate the attempted cyberattack.⁴³ Nevertheless, HC3 did not include actionable cyber threat details in alerts shared across the sector, as provided in HTOC reports. According to the Executive Director for Cybersecurity in the HPH Sector Coordinating Council, the sector's private sector partners would benefit from HC3 providing more actionable cyber threat information that could assist the partners in avoiding cyberattacks.

HC3 has not leveraged actionable threat information collected and reported by HTOC because these two entities do not coordinate their responsibilities for cybersecurity information sharing to the HPH sector. While the HC3 Strategic Plan and HTOC Concept of Operations call for these entities to share cybersecurity information with the HPH sector to protect against cyber threats, these documents do not include specific coordination responsibilities between the two entities. In addition, a senior HTOC official informed us that the entity rarely shares information that is appropriate to share with HC3.

The HHS CISO informed us that HC3 and HTOC coordinate their information sharing efforts during daily situational awareness meetings.⁴⁴ However, according to both the June 2016 and February 2021 *Incident Response and Security Monitoring Standard Operating Procedures*, these meetings are led by the Computer Security Incident Response Center (CSIRC), and are intended to facilitate collaboration among all departments of the CSIRC and provide feedback for any new or pending issues that need to be addressed. Further, the meeting notes that HHS provided from these meetings did not demonstrate coordination between these two entities.

Until HC3 and HTOC formalize coordination of their cybersecurity responsibilities, HHS will continue to miss an opportunity to enhance information sharing to their intended audience.

⁴³An internet protocol address is a unique address that identifies a device on the internet or a local network.

⁴⁴As of June 1, 2021, the HHS CISO in place during this review began serving as the Acting CIO at HHS.

HHS Entities Regularly Shared Cybersecurity Information during COVID-19, but Can Further Improve Collaboration

HHS entities with responsibilities for leading cybersecurity efforts within the department and HPH sector did so through various collaborative groups that it established. As part of these collaborative groups and other information sharing efforts, the HHS entities provided cybersecurity information, guidance, and resources to the department and HPH sector organizations through COVID-19 response efforts. They also coordinated with CISA to share cyber threat information and mitigation tools intended to continually support cybersecurity in the HPH sector during COVID-19.

In addition, HHS entities demonstrated consistency with four of the seven leading practices that GAO identified for collaborating. Those leading practices are to: (1) bridge organizational culture; (2) identify leadership; (3) include relevant participants; and (4) identify resources. However, the entities partially address the remaining three leading practices.

Specifically, while the entities defined goals to establish outcomes and accountability for all the collaborative groups they led, they did not consistently monitor, evaluate, or report their efforts to key decision makers in order to facilitate the identification of areas for improvement. Additionally, the entities did not clearly identify the roles and responsibilities for all the collaborative groups they lead. Further, the entities did not consistently develop written agreements that outlined how all the groups would collaborate. Lastly, for the groups that had written agreements, the HHS entities did not regularly update or monitor their agreements to aid in the success of their collaborative efforts.

HHS Entities Established Various Groups to Support Cybersecurity Collaboration Efforts

The Office of Information Security and ASPR established at least seven cybersecurity-focused collaborative groups to manage their responsibilities to support cybersecurity within the department and to coordinate cybersecurity efforts in the HPH sector. As described in table 4, these groups are intended to facilitate the issuance of policy at HHS, discuss cybersecurity risks and issues within the HPH sector, and share cybersecurity threat information among HHS and the federal healthcare partners, among other things.

Table 3: Roles of the Department of Health and Human Services' (HHS) Cybersecurity-Focused Collaborative Groups Supporting Cybersecurity Management at the Department and Coordination in the Healthcare and Public Health (HPH) Sector

Collaborative Group^a	Role
HHS Chief Information Security Officer Council <i>Led by the Office of Information Security</i>	Functions as the principal forum within HHS to facilitate issuing policy, making risk-based decisions, and addressing enterprise-wide information security issues that impact operating and staff divisions.
HHS Continuous Monitoring and Risk Scoring Working Group <i>Led by the Office of Information Security</i>	Coordinates department-wide continuous monitoring activities. This group was established by the continuous monitoring program, which is intended to provide oversight and compliance with federal continuous monitoring requirements across the department's operating and staff divisions.
Healthcare Threat Operations Center <i>Partnership co-led by HHS Cybersecurity Operations division, Department of Veterans Affairs Cybersecurity Operations Center, and Defense Health Agency</i>	Manages the centralized federal healthcare threat operations center that is intended to improve the computer security and incident response capabilities of its federal partners—the HHS Cybersecurity Operations division, Department of Veterans Affairs Cybersecurity Operations Center, and Defense Health Agency.
HHS Cloud Security Working Group <i>Led by the Office of Information Security</i>	Standardizes security requirements for cloud services and provides subject matter expertise and oversight on cloud security activities, including compliance with federal requirements for cloud security throughout the department.
HHS Cybersecurity Working Group <i>Led by HHS Office of the Assistant Secretary for Preparedness and Response (ASPR)</i>	Serves as the official forum for discussion of cybersecurity issues among the HHS operating and staff divisions in order to improve the security and resilience of the HPH sector's information systems.
Healthcare and Public Health (HPH) Government Coordinating Council's Cybersecurity Working Group <i>Led by ASPR</i>	Coordinates the efforts of federal, state, local, tribal, and territorial HPH partners to enhance critical infrastructure cyber security and resilience and reduce the cyber risk across the entire public health landscape as it pertains to protecting the healthcare community.
Joint HPH Cyber Working Group^b <i>Co-led by ASPR, HHS OCIO, the Food and Drug Administration, and private sector partners^c</i>	Facilitates the public-private partnership between HHS, other federal agencies, including the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency, and private sector partners to develop and encourage adoption of recommendations and guidance for policy and for regulatory and market-driven strategies to facilitate collective mitigation of cybersecurity threats to the HPH sector. ^d

Source: GAO analysis of Department of Health and Human Services' documentation. | GAO-21-403

^aHHS officials in the Office of Information Security informed us that there are several working groups chartered under the CISO Council. Those working groups include the Federal Information Security Modernization Act and Cybersecurity Awareness, Training, and Education working groups. In addition, the six HHS operating divisions that we selected for this review informed us of other working groups, such as the HHS Incident Response Team, HHS IT Strategic Workforce, HHS Cybersecurity Workforce Development, Cyber Threat Coordination working groups, and others. However, the officials in the Office of Information Security did not provide charters for these working groups.

^bThe Joint HPH Cyber Working Group charter that we reviewed is maintained by ASPR. The HPH Sector Coordinating Council maintains a separate charter for its Cybersecurity Working Group, which is made up of the sector's industry partners.

^cThe Food and Drug Administration is the federal agency primarily responsible for evaluating the safety and effectiveness of medical devices. FDA's regulation of medical devices is intended to provide the public with reasonable assurance that medical devices are safe and effective and do not pose a threat to the public's health.

^dAmong other responsibilities, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) has a primary responsibility in coordinating with other government and private-sector partners. As the lead federal agency responsible for overseeing

domestic critical infrastructure protection efforts, CISA's ability to effectively coordinate and consult with its partners—which include other federal agencies; state, local, territorial, and tribal governments; and the private sector—is critical.

HHS Entities Collaborated and Shared Information to Strengthen Cybersecurity During COVID-19 Response

As part of the HHS Office of Information Security's role to manage cybersecurity at the department, the office is responsible for coordinating cybersecurity efforts across the department's operating and staff divisions. In addition, as the sector risk management agency for the HPH sector, HHS is responsible for collaborating with sector partners and coordinating activities to strengthen security and resiliency in the sector. The HHS Office of Information Security and ASPR facilitated collaboration through various collaborative groups to improve cybersecurity at HHS and in the HPH sector during COVID-19. For example, these groups collaborated with the HHS operating and staff divisions and organizations in the HPH sector to provide awareness of ongoing cybersecurity threats and issues and to assist with COVID-19 cyber response efforts.

In November 2020, we reported that, since March 2020, the Office of Information Security and ASPR increased their collaborative efforts to address cybersecurity concerns associated with COVID-19 through the efforts of the following five working groups.⁴⁵

- **Chief Information Security Officer (CISO) Council.** During its April and May 2020 meetings, the CISO Council informed CISOs across HHS of the cybersecurity support (staffing and funding) available to them through DHS in light of the increased COVID-19 related cyber threats.
- **Healthcare Threat Operations Center (HTOC).** In March 2020, HTOC shared cybersecurity threat information among the federal healthcare partners to provide awareness of a phishing campaign that attempted to trick users into thinking that HHS had sent them a legitimate email requesting facemasks and forehead thermometers that were listed in a malicious attachment.
- **HHS Cybersecurity Working Group.** The HHS Cybersecurity Working Group met almost monthly to discuss and coordinate efforts focused on HPH sector cybersecurity. During the group's April 2020

⁴⁵GAO, *COVID-19: Urgent Actions Needed to Better Ensure an Effective Federal Response*, [GAO-21-191](#) (Washington, D.C.: Nov. 30, 2020). We regularly issue government-wide reports on the federal response to COVID-19. For the latest report, see GAO, *COVID-19: Sustained Federal Action Is Crucial as Pandemic Enters Its Second Year*, [GAO-21-387](#) (Washington, D.C.: Mar. 31, 2021). Our next government-wide report will be issued in July 2021 and will be available on GAO's website at <https://www.gao.gov/coronavirus>.

meeting, FDA provided updates on its efforts to engage with the HPH sector's private sector partners for medical device security.

- **Government Coordinating Council's Cybersecurity Working Group.** The Government Coordinating Council's Cybersecurity Working Group collaborated to establish a Telehealth Task Group to address cybersecurity risks to the telehealth industry. The task group, which was formally established in August 2020, met bi-weekly to discuss ongoing telehealth-related activities, such as those led by HHS operating divisions.
- **Joint HPH Sector Cyber Working Group.** In March 2020, the Joint HPH Sector Cyber Working Group collaborated to develop and distribute guidance on managing cybersecurity risks while teleworking, as many organizations moved to remote working.

In March 2021, we reported that, between August and December 2020, the HHS entities—the Office of Information Security and ASPR—continued to collaborate with internal stakeholders and sector partners through the cybersecurity-focused collaborative groups it leads.⁴⁶ Specifically, we described how the groups collaborated on efforts managed by Operation Warp Speed and ongoing efforts to secure telehealth medical services.⁴⁷ For example,

- In August 2020, the Joint HPH Sector Cyber Working Group discussed CISO concerns with Operation Warp Speed due to perceived cyber threats to potential COVID-19 therapeutic and vaccine supply chains.
- In September 2020, the Government Coordinating Council's Cybersecurity Working Group Telehealth Task Group discussed challenges they have experienced in protecting the security and privacy of health information and personal data, as telehealth medical services expanded and information was transferred across networks.

In addition to the collaborative efforts mentioned, the HHS entities provided cybersecurity information, guidance, and resources to the department and HPH sector organizations through COVID-19 response efforts. Specifically, the HHS entities distributed regular cybersecurity information and guidance such as briefings, newsletters, alerts, and notifications across the department and the HPH sector regarding

⁴⁶GAO, *COVID-19: Sustained Federal Action Is Crucial as Pandemic Enters Its Second Year*, [GAO-21-387](#) (Washington, D.C.: Mar. 31, 2021).

⁴⁷The prior administration initiated Operation Warp Speed in May 2020 to accelerate the development, manufacturing, and distribution of COVID-19 vaccines and therapeutics.

cybersecurity preparedness and response efforts. These information products contained cybersecurity awareness, vulnerability, and threat information that informed efforts to address cybersecurity risks during COVID-19 response efforts and are described in appendix II. Additionally, the HHS entities used multiple communication mechanisms to disseminate these cybersecurity-related products during the COVID-19 pandemic. For example:

- The Office of Information Security distributed newsletters internally via email to the HHS operating and staff divisions, and sent the 405(d) Post newsletter and posters to the HPH sector.
- The Computer Security Incident Response Center (CSIRC) sent its cybersecurity notifications throughout the department by email.
- HC3 disseminated its cybersecurity alerts and white papers via email and provided briefings across the department and the HPH sector.
- HTOC sent cyber alert, warning, and threat intelligence information to the federal healthcare partners—HHS, the Department of Veterans Affairs, and the Defense Health Agency via its secure portal, ThreatConnect.⁴⁸
- ASPR sent its newsletters to the HPH sector by email and the Technical Resources Assistance Center and Information Exchange.⁴⁹

Table 5 provides examples of cybersecurity-related products shared by the HHS entities to the department’s operating and staff divisions and HPH sector, as appropriate.

⁴⁸ThreatConnect is a web-based secure portal used by the Healthcare Threat Operations Center to share cybersecurity information with the federal healthcare partners.

⁴⁹The Technical Resources Assistance Center and Information Exchange is a healthcare emergency preparedness information gateway that ensures that all stakeholders—at the federal, state, local, tribal, and territorial government levels; in nongovernmental organizations; and in the private sector—have access to information and resources to improve preparedness, response, recovery, and mitigation efforts. Sponsored by ASPR, the center provides cybersecurity information that is intended to help stakeholders better protect against, mitigate, respond to, and recover from cyber threats, thereby ensuring patient safety and operational continuity.

Table 4: Examples of Cybersecurity-related Products Shared by Department of Health and Human Services (HHS) Entities

HHS entity	Example of information products shared
Office of Information Security	The Office of Information Security's May 2020 <i>HHS Cybersecurity</i> newsletter summarized information on criminal cyber activities related to COVID-19, which was presented by HC3 during a cyber threat briefing. In addition, the office's June 2020 CyberCare newsletter provided information on safely securing mobile devices. As part of its 405(d) activities, the Office of Information Security developed and distributed posters on tips for secure teleworking procedures during COVID-19 and staying cyber diligent during a health crisis in May 2020.
Computer Security Incident Response Center (CSIRC)	In January 2020, CSIRC distributed an alert that described that cyber criminals were using the global fears surrounding the coronavirus to provide guidance on the disease that was included in a malicious email attachment. In July 2020, CSIRC released an advisory notification regarding a critical vulnerability in the Domain Name System server. ^a The notification provided information on how the vulnerability could allow attackers to gain control of their intended target's entire IT infrastructure.
Health Sector Cybersecurity Coordination Center (HC3)	In May 2020, HC3 provided a threat briefing on COVID-19's effects on HIPAA compliance regulations for providers leveraging technology platforms to facilitate telehealth services during the pandemic. ^b In addition, HC3 distributed information on malware and mitigation strategies through its sector alerts. ^c
Healthcare Threat Operations Center (HTOC)	In April 2020, HTOC sent an alert to the federal healthcare partners describing a phishing campaign where email recipients were sent an email that requested them to open a malicious attachment to provide a quote for a list of medical equipment, such as facemasks and thermometers that were needed in response to COVID-19.
Office of the Assistant Secretary for Preparedness and Response (ASPR)	ASPR's April 2020 <i>Healthcare and Public Health (HPH) Sector Highlights Cybersecurity Edition</i> newsletter included joint cybersecurity guidance on teleworking during COVID-19 from the American Medical Association and the American Hospital Association that was intended to help hospitals and providers strengthen their security measures. In September 2020, ASPR also shared information on malware and related mitigation strategies through its Technical Resources, Assistance Center, and Information Exchange gateway.

Source: GAO analysis of Department of Health and Human Services' documentation | GAO-21-403

^aThe Domain Name System server translates domain names to Internet Protocol addresses to enable access to internet resources by user-friendly domain names rather than Internet Protocol addresses. An Internet Protocol address is a unique address that identifies a device on the Internet or a local network.

^bTelehealth is a clinical service provided remotely via telecommunications systems with audio and video equipment permitting two-way, real-time interactive communication between the patient and the healthcare provider.

^cMalware is defined as software designed to carry out annoying or harmful actions.

Senior officials from six selected HHS operating divisions confirmed that the Office of Information Security uses various products, such as newsletters, briefings, alerts, and notifications via emails and meetings to share cybersecurity information.⁵⁰ In addition, the officials said that they

⁵⁰The six selected operating divisions were the Food and Drug Administration, Centers for Medicare and Medicaid Services, Centers for Disease Control and Prevention, Health Resource and Services Administration, Substance Abuse and Mental Health Services Administration, and Agency for Health Research and Quality.

were satisfied with the Office of Information Security's efforts to share information to manage cybersecurity throughout the department.

In addition to information sharing, and consistent with their defined cybersecurity responsibilities, the HHS entities provided resources to support the department and the HPH sector's cybersecurity preparedness and response efforts during the pandemic, as described in the next section.

Resources provided to the HHS operating and staff divisions through the DHS Continuous Diagnostic and Mitigation Program.

The HHS Office of Information Security provided cybersecurity advisory support as various operating and staff divisions across the department harnessed new technologies and tools to support COVID-19 efforts. For example, the officials noted that the HHS OCIO engaged with DHS through the Continuous Diagnostics and Mitigation program to obtain additional support, such as additional staff and funding, tools, and technologies to increase cybersecurity protection throughout the department.⁵¹ To do so, the HHS Office of Information Security coordinated with the CISOs of the HHS operating divisions to understand their resource needs.

Officials from one of the six selected operating divisions informed us that the coordination with DHS was beneficial, since it allowed for additional resources without disrupting ongoing efforts to identify and implement cybersecurity priorities. The officials from five of the six selected operating divisions noted that they received cybersecurity support, including guidance, funding, and staff from the Office of Information Security. Specifically, officials from two of the five operating divisions said that they received additional staff, two others reported receiving cybersecurity guidance, and another obtained funding to strengthen cybersecurity defenses during COVID-19.

Resources provided to the HPH sector through the COVID-19 Entity Specific Cyber Watch Program. HHS coordinated with CISA to

⁵¹DHS developed the Continuous Diagnostic and Mitigation program in 2013 to strengthen the cybersecurity of government networks and systems by providing tools to agencies to support the continuous monitoring of their networks. The program is intended to allow federal agencies to automate network monitoring, correlate and analyze security-related information, and enhance risk-based decision making at both the individual agency and federal levels.

disseminate cyber threat information and mitigation tools to support cybersecurity in the HPH sector during COVID-19. For example, as part of the COVID-19 Entity Specific Cyber Watch program, ASPR, in coordination with HC3, CISA, and the FBI, conducted weekly meetings to identify and notify critical organizations engaged in the development of COVID-19 therapeutics and vaccines that need additional protection during the nation's continued response to the pandemic.⁵² The program offers cybersecurity support through engagements to ensure that the identified entities are not impacted or interrupted by cyber threats. According to HHS officials, the COVID-19 Entity Specific Cyber Watch program began in March 2020 and was still ongoing as of March 2021.

Collaboration with DHS to provide assistance to the HPH sector.

According to a CISA official, since the pandemic started, HC3 has collaborated with DHS to provide HPH sector organizations access to CISA's Cyber Hygiene Vulnerability Scanning and Web Application Scanning services.⁵³ Further, since March 2020, HC3 has routinely provided information on cybersecurity threats, vulnerabilities, and incidents to CISA. According to CISA officials, the department received cybersecurity information sharing products from HC3 and disseminated the information more broadly to federal, state, and local partners, private industries, critical infrastructure partners, and international partners through various information sharing platforms, including the Homeland Security Information Network.⁵⁴

HHS Entities Fully Demonstrated Most, but Not All Leading Practices for Collaboration

In our prior work, we identified the following seven leading practices that collaborative mechanisms, such as working groups and councils, can benefit from using.⁵⁵

⁵²The COVID-19 Entity Specific Cyber Watch program executed and coordinated government-wide cyber engagements in support of HPH sector entities that were developing and testing COVID-19 therapeutics and vaccines.

⁵³The scanning services are free and assist organizations with identifying vulnerabilities and misconfigurations on their external network, which could be subject to attack and exploitation from malicious actors.

⁵⁴The Homeland Security Information Network is a web-based platform operated by the Department of Homeland Security to facilitate sensitive but unclassified information sharing and collaboration among federal, state, local, tribal, and private sector organizations.

⁵⁵[GAO-12-1022](#)

-
- **Outcomes and accountability** addresses whether short- and long-term outcomes have been clearly defined, and the extent tracking and monitoring of progress in achieving outcomes has been performed.
 - **Bridging organizational cultures** includes identifying the missions and cultures of the participating organizations in the collaborative groups.
 - **Leadership** involves designating an individual who will lead the collaborative groups.
 - **Clarity of roles and responsibilities** addresses whether the collaborative groups have clarified roles and responsibilities.
 - **Participants** includes ensuring that all relevant participants are involved in the collaborative groups.
 - **Resources** involves leveraging relevant staff and IT resources to support the operations of the collaborative groups.
 - **Written guidance and agreements** includes documenting the collaborative groups' agreement regarding how they will collaborate, and determining ways to continually update and monitor these agreements.

These leading practices provide actions for agency officials to consider when working collaboratively. For example, agency officials should consider whether the collaborative groups have defined goals and whether they track and monitor progress on meeting the goals, and whether the collaborative groups have documented and regularly updated written agreements on how they will be collaborating.

The HHS Office of Information Security and ASPR led at least seven collaborative groups to fulfill their cybersecurity responsibilities. The extent to which each of the entities demonstrated consistency with each of the seven leading practices for collaborating is summarized in table 6.

Table 5: Examples of the Department of Health and Human Services’ Cybersecurity Collaborative Groups’ Actions that were Generally Consistent with the Leading Practices for Collaboration

Leading practices for collaboration	Demonstrated leading practice	Examples of actions taken by the cybersecurity collaborative groups
Outcomes and accountability	●	<p>Although all seven collaborative groups defined goals, only two monitored and tracked their progress towards meeting the goals. For example:</p> <ul style="list-style-type: none"> • The Healthcare Threat Operations Center (HTOC) collected several metrics to monitor its progress. • The Joint Healthcare and Public Health Cyber Working Group reported on the progress of several of its task groups during a working group meeting.
Bridging Organizational Culture	●	<p>The seven collaborative groups included participants that have responsibilities aligned to the mission of the groups. For example:</p> <ul style="list-style-type: none"> • The HHS Chief Information Security Officer Council included the Chief Information Security Officers across the operating divisions of the department that have significant responsibilities for implementing cybersecurity at their respective operating division. • The HHS Cybersecurity Working Group included participants from HHS staff and operating divisions that engage in regulating cybersecurity matters, promoting cybersecurity, engaging in cybersecurity research and development, and providing cybersecurity technical assistance, among other things.
Leadership	●	<p>The seven collaborative groups identified individuals who are leading or co-leading the groups. For example:</p> <ul style="list-style-type: none"> • The HHS Chief Information Security Officer Council, HHS Continuous Monitoring and Risk Scoring Working Group, and Cloud Security Working Group designated the Chief Information Security Officer (CISO) or CISO’s designee as the chair of these groups. • The Director of ASPR’s Critical Infrastructure Protection Division designated the division’s Senior Cybersecurity Advisor as the chairperson of the HHS Cybersecurity Working Group and the HPH Government Coordinating Council’s Cybersecurity Working Group.
Clarity of roles and responsibilities	●	<p>Six of the seven collaborative groups defined roles and responsibilities for the overarching group and the members that participate in the group. For example:</p> <ul style="list-style-type: none"> • The Continuous Monitoring and Risk Scoring Working Group defined roles and responsibilities for several of its members, as well as the entire group. • While the Government Coordinating Council’s Cybersecurity Working Group’s current charter defines the role for the working group, it does not include a description of the group’s responsibilities.
Participants	●	<p>The seven collaborative groups included relevant participants in their collaboration meetings. For example:</p> <ul style="list-style-type: none"> • The HHS Chief Information Security Officer Council’s members included the Chief Information Security Officers from the HHS operating divisions. The council may invite subject matter experts to the meetings as appropriate. • The HHS Cybersecurity Working group included various representatives from various operating and staff divisions, such as the Centers for Disease Control and Prevention, Food and Drug Administration (FDA), Office for Civil Rights, and Office of the National Coordinator for Health Information Technology, as standing members.

Leading practices for collaboration	Demonstrated leading practice	Examples of actions taken by the cybersecurity collaborative groups
Resources	●	<p>The seven collaborative groups identified human and leveraged IT resources to support collaborating. For example:</p> <ul style="list-style-type: none"> In addition to the human participants that support the group as described above, the HHS Chief Information Security Officer Council used teleconference tools for meetings not held in-person. The Joint HPH Cyber Working Group’s members included ASPR, the HHS Office of the Chief Information Officer, and FDA, along with industry partners. The Joint HPH Cyber Working Group charter states that the members of the group are required to use the DHS Homeland Security Information Network for verification and communication purposes.
Written guidance and agreements	◐	<p>Six of the seven collaborative groups documented how they would collaborate in a charter or concept of operations document, but only one monitored and updated their process for collaborating. Specifically:</p> <ul style="list-style-type: none"> HTOC’s concept of operations document states that HTOC intends to meet annually to address evolving cyber threats, and the HTOC analysts will meet bi-weekly and the leadership will conduct monthly calls to discuss significant issues identified by the HTOC team members. HTOC’s concept of operations had been updated several times since the initial creation of the document—twice in 2015 and again in 2020—to reflect changes in the participating organizations and to define terms to be used within the document.

Legend: ● demonstrated leading practice ◐ partially demonstrated leading practice ○ did not demonstrate leading practice.

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

Note: The charters of the working groups did not describe any financial resources needed. We did not obtain funding resources data from the working groups.

The HHS Office of Information Security and ASPR partially demonstrated the leading practices of three of the seven leading practices that we have identified for collaborating—outcomes and accountability, clarity of roles and responsibilities, and written agreements. The extent to which each of the entities demonstrated consistency of these three leading practices for collaborating is summarized in table 7.

Table 6: Extent to Which the Department of Health and Human Services’ Cybersecurity Collaborative Groups Demonstrated Leading Practices for Collaboration

Collaborative group	Outcomes and accountability	Clarity of roles and responsibility	Written agreements
HHS Chief Information Security Officer Council	◐	●	◐
HHS Continuous Monitoring and Risk Scoring Working Group	◐	●	◐
Healthcare Threat Operations Center	●	●	●
HHS Cloud Security Working Group	◐	●	◐
HHS Cybersecurity Working Group	◐	●	◐
HPH Government Coordinating Council’s Cybersecurity Working Group	◐	○	◐

Collaborative group	Outcomes and accountability	Clarity of roles and responsibility	Written agreements
Joint HPH Cyber Working Group	●	●	●

Legend: ● fully demonstrated leading practice ● partially demonstrated leading practice ○ did not demonstrate leading practice.

HHS = Department of Health and Human Services; HPH = healthcare and public health.

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

Outcomes and accountability

Based on our leading collaboration practices, collaborative groups, such as working groups and councils, benefit from having clear goals that establish organizational outcomes and accountability. Specifically, by establishing a goal based on what the group shares in common, a collaborative group can shape its vision and define its purpose. Additionally, agencies that establish a means to monitor, evaluate, and report the results of collaborative efforts to the key decision makers can better facilitate the identification of areas for improvement.⁵⁶

HHS entities responsible for coordinating cybersecurity among the department and HPH sector organizations defined goals for the seven cybersecurity-focused collaborative groups. Table 8 identifies the collaborative groups led by the HHS Office of Information Security and ASPR and their respective goals.

Table 7: Goals of Collaborative Groups led by the HHS Office of Information Security and Office of the Assistant Secretary for Preparedness and Response (ASPR)

Collaborative Group	Goals
The Department of Health and Human Services (HHS) Chief Information Security Officer Council	<ul style="list-style-type: none"> Address and evaluate the information security needs of the department as defined by HHS policy and federal requirements and guidance. Establish a strategic vision and recommend operational actions that ensure interoperability and transparency; promote data, information, and knowledge sharing; foster departmental collaboration; and support mandates for HHS information security. Serve as a forum for reviewing risk-based decisions to improve the overall information security posture of HHS.
HHS Continuous Monitoring and Risk Scoring Working Group	To enable HHS operating divisions to own, develop, and implement individual yet coordinated continuous monitoring implementation plans that support the HHS vision of maintaining near real time awareness of the department-wide information security risk profile.

⁵⁶GAO, *Results-Oriented Government: Practices That Can Help Enhance and Sustain Collaboration among Federal Agencies*, [GAO-06-15](#) (Washington, D.C.: Oct. 21, 2005).

Collaborative Group	Goals
Healthcare Threat Operations Center	To maintain a cyber threat common operational picture and provide federal healthcare partners with situational awareness that strengthens the security and resilience of the federal healthcare sector IT systems, networks, and critical infrastructure.
HHS Cloud Security Working Group	<ul style="list-style-type: none"> • Provide guidance on Federal Risk and Authorization Management Program (FedRAMP) compliance throughout the department.^a • Facilitate collaboration across HHS on FedRAMP, cloud security issues, best practices, and lessons learned. • Provide a forum for visibility and consultation on cloud security policies and procedures, practices, memoranda, and guidance. • Ensure consistent execution of cloud security related activities, policies, and requirements. • Serve as a forum for discussing and advising on specific cloud security compliance. • Coordinate and provide cloud security subject matter expertise to other HHS councils, as needed.
HHS Cybersecurity Working Group	<ul style="list-style-type: none"> • Coordinate HHS input on policy proposals from the Executive Office of the President, oversight organizations, federal agencies, and others related to cybersecurity within the scope of its authority. • Provide high-level coordination for operation activities related to HHS's mission. • Coordinate with various stakeholders such as private sector, state, local, tribal, and territorial partners for outreach activities. • Provide a forum for sharing information on departmental cybersecurity activities to identify opportunities for enhanced coordination. • Discuss potential gaps in policies and programs supporting HPH sector cybersecurity and provide recommendations to address those gaps.
Healthcare and Public Health (HPH) Sector Government Coordinating Council's Cybersecurity Working Group	<ul style="list-style-type: none"> • Share cybersecurity information across the agencies as it relates to the HPH sector. • Meet the objectives of various federal laws and policies that seek to reduce vulnerabilities and hasten response and recovery efforts related to the HPH sector, among other things. • Identify authorities and capabilities that agencies can employ to support the cybersecurity efforts of critical infrastructure organizations in support of major cyber incidents in the HPH sector. • Align healthcare-related cybersecurity partnership activities and approaches.

Collaborative Group	Goals
Joint HPH Cyber Working Group	<ul style="list-style-type: none"> • Develop an ongoing discussion on incorporating new technology into healthcare and public health practices without compromising patient safety or access by individuals to their data, as required by law. • Analyze existing and encourage new information-sharing activities regarding threat information and security incidents among government and private sector organizations, and develop actionable incident management and cybersecurity guidance for various audiences. • Support development of the HPH sector risk assessment tool. • Coordinate the development of a tailored, sector-wide HPH implementation guide of the National Institute of Science and Technology's (NIST) Cybersecurity Framework, leverage existing documents and efforts within and beyond the sector partners, and develop supplemental guidance for the various levels of users. • Collaborate with NIST, the Department of Homeland Security, and federal and private sector partners to develop guidelines, best practices, methodologies, procedures, and processes that are voluntary, consistent with NIST standards and federal requirements, and are updated on regular basis.

Source: GAO analysis of information provided by the Department of Health and Human Services. | GAO-21-403

⁸The Office of Management and Budget established the Federal Risk and Authorization Management Program in 2011. The program is intended to provide a standardized approach for selecting and authorizing the use of cloud services that meet federal security requirements.

Although HHS entities defined goals for each of the seven collaborative groups, the department did not consistently monitor, evaluate, or report on the progress of the groups to the decision makers—agency leaders and managers—to facilitate the identification of areas for improvement. Specifically, HHS tracked and monitored the progress made toward meeting goals for two of the seven groups.

HTOC collected several metrics to monitor progress toward established goals, such as the number of posts⁵⁷ generated within ThreatConnect, the number of indicators⁵⁸ added each month, and the threat models established by the center.⁵⁹ The officials stated that these metrics are compiled into a quarterly report that is provided to the Director of Cyber Security Operations.

The Joint HPH Cyber Working Group monitored and reported on the progress of goals established by its task groups. For example, during its

⁵⁷Posts are generated when HTOC analysts enter data into ThreatConnect. This can include an overview of the campaign and set of indicators.

⁵⁸The indicators are shared items, such as Internet Protocol addresses, host names, and email addresses, which can be used to identify recurring malicious activity.

⁵⁹ThreatConnect is a secure portal intended to share cyber alert, warning, and threat intelligence with the federal healthcare partners.

October 2020 “All-Clicks” meeting—which ASPR officials informed us occurs twice a year—the group leaders reported on the performance of their respective task groups. Specifically, leaders for the Future Gazing, Healthcare Tech Risk Analysis, Telemedicine, Workforce Development, and Medical Device Security task groups reported on the objectives, outcomes, milestones, and/or deliverables, including their status and estimated completion dates for the groups. Additionally, ASPR officials informed us that the working group monitors and reports on the progress of the task groups on a weekly basis through a web-based collaborative platform. However, the Executive Director for Cybersecurity in the HPH Sector Coordinating Council informed us that the process to measure progress in the working group could be more structured and strategic among HHS and the private sector partners.

However, the other five groups—the HHS CISO Council, Continuous Monitoring and Risk Scoring Working Group, Cloud Security Working Group, HHS Cybersecurity Working Group, and Government Coordinating Council’s Cybersecurity Working Group—did not have mechanisms in place to monitor and evaluate progress. While the charters of these five groups defined goals, none described a process for monitoring, evaluating, or reporting progress towards meeting the goals.

Although the HHS Deputy CISO stated that the regular meetings for the CISO Council, Continuous Monitoring and Risk Scoring Working Group, and Cloud Security Working Group demonstrated the fulfillment of the groups’ goals, HHS did not establish any mechanisms to monitor and report on the progress of these groups.⁶⁰ In addition, while the meetings demonstrated that the working groups intended to collaborate as agreed upon in the charters, the fact that they occurred is not a sufficient metric for measuring the performance of the working groups against their defined goals.

Further, the Director of ASPR’s Critical Infrastructure Protection Division stated that the office was limited in its ability to monitor and report on the progress of meeting defined goals for the HHS Cybersecurity Working Group and Government Coordinating Council’s Cybersecurity Working Group due to resource constraints related to staffing. The official further noted that ASPR’s current resources for cybersecurity are shared with its overall responsibility for HPH sector’s protection efforts, which are

⁶⁰As of June 1, 2021, the HHS Deputy CISO in place during this review began serving as the Acting CISO at HHS.

prioritized over efforts to monitor and report on the progress of the groups. However, monitoring and reporting on the progress of the working groups, which are intended to support ASPR's protection efforts, would help ensure that those efforts are effectively and efficiently using the time and resources of group participants.

Without a defined process to monitor and evaluate the efforts of each collaborative group, HHS has reduced assurance that the groups are conducting their efforts effectively. In addition, HHS will not have the information it needs to identify and inform key decision makers on areas of improvement for both policy and operational effectiveness of the groups.

Clarity of roles and responsibilities

One of the leading practices we have identified to be helpful in enhancing collaboration is clarifying roles and responsibilities of the collaborative groups. HHS entities identified roles and responsibilities in their charters and concept of operations, for six of its seven collaborative groups. For example:

- **CISO Council.** The charter for the council described the responsibilities of the council, which include establishing department-wide information security best practices; sharing information on potential security threats and recommended safeguards to the department's information security stakeholders; and recommending the acquisition of security technologies for the department, among other things.
- **The Continuous Monitoring and Risk Scoring Working Group.** The charter of the working group outlined the roles and responsibilities of the HHS Continuous Monitoring Chair, Continuous Monitoring and Risk Scoring Work Group's Coordinator, the members of the group, as well as for the working group. According to the charter, the working group is responsible for monitoring the progress of the HHS operating divisions' continuous monitoring programs and implementation plans by using CyberScope, and sharing continuous monitoring best practices and lessons learned to the operating divisions, among other things.⁶¹

⁶¹CyberScope is the reporting system managed by the Department of Homeland Security through which agencies are to report their FISMA-related performance metrics.

-
- **HTOC.** The concept of operations described the responsibilities of the center, which included establishing and maintaining a centralized federal healthcare threat operations center that is intended to share information concerning any external or internal cyber threats or incidents that may impact the ability of the federal healthcare partners to perform their missions.
 - **Cloud Security Working Group.** The work group's charter outlined the roles and responsibilities of the Cloud Security Working Group Chair and Coordinator, the HHS operating division CISO Designee, the HHS Cloud Security team members, and the members of the group. The members of the work group are responsible for supporting the group's vision and goals, and sharing expertise and guidance to support the vision of the group, among other things.
 - **HHS Cybersecurity Working Group.** The working group's charter described the responsibilities of the working group, which included completing activities to coordinate policy and stakeholder engagement, sharing information, and performing gap analysis and prioritization, among other things.
 - **Joint HPH Cyber Working Group.** The work group's charter outlined various task groups and their associated responsibilities that are intended to meet the mission of the working group. For example, the Future-gazing task group is responsible for developing an ongoing conversation on how to incorporate new technology into HPH industry practice without compromising patient safety or individual's access to their data.

ASPR drafted a charter for the remaining collaborative group—the HPH Sector Government Coordinating Council Cybersecurity Working Group—that described the mission, objective, and members of the working group. However, ASPR did not identify the roles and responsibilities for the group in its charter. Officials informed us that the draft document dated March 2020, is the current charter for the group and, as of March 2021, the group had not finalized the charter. Until ASPR defines the roles and responsibilities of the HPH Sector Government Coordinating Council Cybersecurity Working Group, ASPR remains unclear of who is accountable for implementing what the group is trying to accomplish.

Written guidance and agreements

According to our leading collaboration practices, agencies that articulate their collaborative agreements in formal documents that are signed by senior officials can strengthen their commitment to working collaboratively. In addition, regularly updating and monitoring those

written agreements can enhance the effectiveness of the collaborative efforts.⁶²

HHS entities documented how they would collaborate in written agreements, such as charters and a concept of operations, for six of its the seven collaborative groups. For example:

- The CISO Council charter stated that it will coordinate information security policy, practices, and procedures at the department level and within the operating divisions. To do this, the charter stated that there will be standing monthly meetings and emergency meetings to address time-critical topics. Additionally, the charter included a description of the responsibilities of the council, the specific role of the CISO Council's chair, and administrative duties, such as meeting and voting requirements.
- The Continuous Monitoring and Risk Scoring Working Group charter stated that the working group is to meet regularly and on an ad-hoc basis to support the department's continuous monitoring functions. The charter also described the responsibilities of key stakeholders, such as the working group's chair and coordinator, and provided expectations for its members.
- The HTOC concept of operations document stated that HTOC intends to meet annually to address evolving cyber threats. Additionally, the concept of operations stated that the HTOC analysts will meet bi-weekly and the leadership will conduct monthly calls to discuss significant issues identified by the HTOC team members. The HTOC concept of operations also described various aspects of the center's mission execution, to include its operations, process, and communications.
- The Cloud Security Working Group charter noted that the working group will meet quarterly and on an ad-hoc basis to facilitate communication and collaboration on cloud security activities throughout the department. The charter also described roles and responsibilities of the work group's chair, coordinator, operating divisions' CISOs, and cloud security team members.
- The HHS Cybersecurity Working Group charter stated that the working group intends to meet no more than weekly and no less than monthly to discuss cybersecurity issues to improve the security and resilience of the HPH sector's information systems. Additionally, the

⁶²[GAO-12-1022](#)

charter stated that the working group may schedule ad hoc meetings, as necessary, to address urgent issues or incidents. The charter also described coordination, stakeholder engagement, and information sharing activities of the working group.

- The Joint HPH Cyber Working Group charter included tasks related to information sharing and risk management, among other things, that the working group or task groups intended to work on while the charter is active. The charter noted that each task is implemented by an associated task group that is led by a government official and/or private sector individual. According to the charter, the task groups will meet as needed to manage tasks.

The draft charter for the HPH Sector Government Coordinating Council Cybersecurity Working Group did not describe how the working group's members would collaborate. Additionally, while the Director of ASPR's Critical Infrastructure Protection Division informed us that the working group meets monthly, the draft charter did not describe the expected frequency of the working group to communicate to foster a collaborative environment.

Further, although HHS had documented agreements for collaboration for six of the seven collaborative groups, only one group—HTOC—had monitored and updated its agreement. Specifically, the concept of operations had been updated several times since the initial creation of the document—twice in 2015 and again in 2020—to reflect changes in the participating organizations and to define terms to be used within the document. HTOC officials informed us that the concept of operations was not updated between 2016 and 2019 because HTOC leadership did not identify any necessary updates.

Of the six remaining collaborative groups that had not monitored and updated their agreements:

- The Office of Information Security had not updated the charter for the HHS CISO Council to reflect federal cybersecurity requirements established since the charter's approval in January 2013. Specifically, the charter stated that the council serves as a forum for reviewing risk-based decisions to improve the overall information security posture of the department. However, the document did not include federal requirements included in Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, which sets requirements for managing cybersecurity

risk as an executive branch enterprise.⁶³ In addition, the charter referenced the *Federal Information Security Management Act of 2002*, which was largely superseded by the *Federal Information Security Modernization Act of 2014* in December 2014. Further, the office had not updated the CISO Council's charter since receiving a signature by the prior CISO in January 2013. As a result, the charter does not include an authorizing signature from the current CISO, who had been serving in the position since April 2018.

- The charter for the Continuous Monitoring and Risk Scoring Working Group, dated December 2013, stated that the continuous monitoring program was intended to maintain near real-time awareness of the department-wide information security risk profile. However, the charter did not reflect the government's current priorities for continuous monitoring, such as those prescribed in the *National Cybersecurity Protection Advancement Act of 2015*. The act requires agencies to protect their networks through the use of federal intrusion prevention and detection capabilities.⁶⁴ In addition, the office had not updated the charter since receiving a signature by the prior CISO in December 2012. As a result, the charter does not include an authorizing signature from the current CISO, who had been serving in the position since April 2018.
- The Cloud Security Working Group charter, dated March 2020, did not have an authorizing signature from the CISO, who is the chair of the working group. HHS OCIO officials informed us that the Cloud Security Working Group charter is currently being updated, but did not provide an estimated time frame for completion.
- The HHS Cybersecurity Working Group provided a charter dated January 2017 that includes a signature from the prior Acting HHS Deputy Secretary. The charter had not been updated to include an authorizing signature from the former Deputy Secretary who held that position between October 2017 and January 2021. ASPR officials stated that they update the charter on an ad-hoc basis, and provided documentation showing that they are currently taking steps to update

⁶³Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, directs agencies to manage cybersecurity risks to the federal enterprise by, among other things, using the NIST *Framework for Improving Critical Infrastructure Cybersecurity*.

⁶⁴The act is a subtitle of the *Cybersecurity Act of 2015* that is Division N of the *Consolidated Appropriations Act, 2016*, Pub. L. No. 114-113, § 223(b), div. N, title II, subtitle B, 129 Stat. 2242, 2966 (Dec. 18, 2015).

the charter. However, they did not provide an estimated time frame for completion.

- ASPR had not finalized the charter for the HPH Sector Government Coordinating Council Cybersecurity Working Group. Officials informed us that the draft document dated March 2020 is the current charter for the group. A senior official from ASPR stated that the office had received feedback as part of the Healthcare Ready project to accelerate finalizing a formal charter for the working group by the beginning of fiscal year 2021.⁶⁵ However, as of March 2021, the collaborative group had not finalized the charter to reflect the approval of the authorized officials leading the working group.
- ASPR did not have a valid charter for the Joint HPH Cyber Working Group, which is dated for fiscal year 2017-2018, despite the charter noting that it would be valid only through the end of fiscal year 2018. Additionally, the charter did not have signatures that reflect the approval from the senior officials leading the working group—the sector and government coordinating councils’ co-chairs and sector risk management agency lead.

HHS OCIO officials stated that the department revises the charters when the intent or function of the working groups change, or when otherwise deemed necessary. They added that, since no significant changes occurred within the CISO Council and the Continuous Monitoring and Risk Scoring Working Group, the charters for these two collaborative groups had not been updated. In addition, the Director of ASPR’s Critical Infrastructure Protection Division stated that the office was unable to regularly update the charters for the remaining three groups—the Government Coordinating Council’s Cybersecurity Working Group, the HHS Cybersecurity Working Group, and the Joint HPH Cyber Working Group—due to resource constraints.

However, without updating and monitoring the written agreements for the CISO Council and Continuous Monitoring and Risk Scoring Working Group, the HHS Office of Information Security has reduced assurance that the groups are collaborating in a manner consistent with the recent federal cybersecurity requirements aimed at improving the overall information security posture of the department. Additionally, until ASPR finalizes the charter for the HPH Government Coordinating Council Cybersecurity Working Group to include a description of how the group

⁶⁵Healthcare Ready is a national nonprofit organization that facilitates public and private sector collaboration to minimize the impact of disruptions to community health.

will collaborate, ASPR cannot strengthen collaborative participation within the working group, which officials identified as a challenge.

Further, by not obtaining authorizing signatures from the senior officials for the charters of the CISO Council, Continuous Monitoring and Risk Scoring Working Group, Cloud Security Working Group, Joint HPH Cyber Working Group, and HHS Cybersecurity Working Group, the HHS Office of Information Security and ASPR may lack sufficient oversight by the relevant managing officials. This, in turn, could lead to ineffective collaboration among the groups.

Conclusions

HHS has effectively assigned responsibilities for carrying out its roles in managing cybersecurity within the department and supporting cybersecurity efforts in the HPH sector. In addition, HHS has clearly defined the responsibilities of its entities to carry out their roles in managing the department's cybersecurity program and providing assistance to the HPH sector.

While HHS clearly defined the cybersecurity information sharing responsibilities for HC3 and HTOC, HC3 did not obtain actionable cyber threat information from HTOC to strengthen its information sharing responsibilities to the sector. This is due, in part, to HHS not describing coordination between HC3 and HTOC in the plans and procedures defining their responsibilities for cybersecurity information sharing. Until HC3 and HTOC formalize coordination of their cybersecurity information sharing responsibilities, sector partners will likely be without important threat information.

As part of its seven collaborative groups and information sharing efforts, the HHS entities regularly collaborated and provided cybersecurity information, guidance, and resources to stakeholders in the department and HPH sector for cybersecurity preparedness and response efforts during COVID-19. They also coordinated with CISA to share cyber threat information and mitigation tools intended to continually support cybersecurity in the HPH sector during COVID-19. In addition, the Office of Information Security and ASPR demonstrated consistency with four of the seven leading collaboration practices that we have identified in the seven collaborative groups it led. The entities partially addressed the remaining three leading collaboration practices. HHS actions to fully demonstrate the remaining three practices can help ensure that it is improving cybersecurity within the department and HPH sector.

Recommendations for Executive Action

We are making the following seven recommendations to HHS:

The Secretary of HHS should direct the Chief Information Officer to coordinate cybersecurity information sharing between the Health Sector Cybersecurity Coordination Center and Healthcare Threat Operations Center. (Recommendation 1)

The Secretary of HHS should direct the Chief Information Officer to monitor, evaluate, and report on the progress and performance of the HHS Chief Information Security Officer Council, Continuous Monitoring and Risk Scoring Working Group, and Cloud Security Working Group. (Recommendation 2)

The Secretary of HHS should direct the Assistant Secretary for Preparedness and Response to monitor, evaluate, and report on the progress and performance of the Government Coordinating Council's Cybersecurity Working Group and HHS Cybersecurity Working Group. (Recommendation 3)

The Secretary of HHS should direct the Chief Information Officer to regularly monitor and update written agreements describing how the HHS Chief Information Security Officer Council, Continuous Monitoring and Risk Scoring Working Group, and Cloud Security Working Group will facilitate collaboration, and ensure that authorizing officials review and approve the updated agreements. (Recommendation 4)

The Secretary of HHS should direct the Assistant Secretary for Preparedness and Response to ensure that authorizing officials review and approve the charter describing how the HHS Cybersecurity Working Group will facilitate collaboration. (Recommendation 5)

The Secretary of HHS should direct the Assistant Secretary for Preparedness and Response to (1) finalize written agreements that include a description of how the Government Coordinating Council's Cybersecurity Working Group will collaborate, (2) identify the roles and responsibilities of the working group, (3) monitor and update the written agreements on a regular basis, and (4) ensure that authorizing officials leading the working group approve the finalized agreements. (Recommendation 6)

The Secretary of HHS should direct the Assistant Secretary for Preparedness and Response to update the charter for the Joint Healthcare and Public Health Cybersecurity Working Group for the

current fiscal year and ensure that authorizing officials leading the working group review and approve the updated charter. (Recommendation 7)

Agency Comments and Our Evaluation

HHS provided written comments on a draft of this report. In its comments, which are reproduced in appendix III, the department concurred with six recommendations that we made to address deficiencies in its efforts to collaborate on cybersecurity with internal stakeholders and external HPH sector partners. The department did not concur with one recommendation.

HHS stated that it is currently taking action to address the six recommendations with which the department agreed. Specifically, regarding our recommendations to improve the HHS-led collaborative groups intended to address internal cybersecurity (recommendations 2 and 4), the department stated that it plans to take a number of actions. These actions include convening a brainstorming session to consider applicable methods to monitor, evaluate, and report on the progress and performance of the HHS CISO Council. In addition, the department stated that it is in the process of updating, finalizing, and obtaining leadership approval for the Cloud Security Working Group charter.

With regard to our recommendations to improve the HHS-led collaborative groups intended to address cybersecurity in the HPH sector (recommendations 3, 5, 6 and 7), the department said it plans to take a number of actions. These include a joint effort between ASPR and OCIO to revise the charter for the Government Coordinating Council's Cybersecurity Working Group. The department also stated that ASPR and OCIO are currently implementing efforts to restructure the HHS Cybersecurity Working Group to increase operational efficiency and collaboration across the HHS operating divisions.

HHS did not concur with our recommendation to coordinate cybersecurity information sharing between HC3 and HTOC (recommendation 1) for several reasons. Specifically the department stated that:

- There is close coordination between HC3 and HTOC that takes into consideration the stakeholders and agreements between relevant partners and stakeholders.
- It does not believe any duplication exists in the information sharing disseminated by HC3 and HTOC.

-
- Due to the high-level of fidelity and sensitivity that surrounds federal intelligence data and the HTOC federal partner cybersecurity operational data, HTOC partners do not share information outside the partnership without expressed permission and authorization of the originating agency.

However, as we reported, HHS documentation that described HC3's and HTOC's roles and responsibilities did not include specific coordination responsibilities between the two entities. Further, the department did not provide additional documentation demonstrating coordination between these entities. According to leading practices for collaboration, which includes coordination, clarifying roles and responsibilities can be helpful for enhancing collaborative efforts. In addition, articulating agreements to collaborate in formal documents can strengthen the commitment to working collaboratively.

Regarding duplication in the information products disseminated by HC3 and HTOC, we reported that HHS had clearly defined the responsibilities for HC3 and HTOC in documentation. However, given the role of these entities to strengthen cybersecurity in the HPH sector, we reported that HC3 and HTOC could enhance cybersecurity information sharing to the sector by coordinating their efforts. Coordination between these two entities for cybersecurity information sharing could potentially strengthen cybersecurity mitigation efforts among the HPH sector's private partners. A private-sector representative in the HPH sector informed us that they could benefit from more actionable cyber threat information from HC3 to assist with avoiding cyberattacks.

Further, in regard to HHS's assertion about the high-level of fidelity and sensitivity of the cybersecurity information HTOC receives, federal guidance issued by the Office of the Director of National Intelligence, DHS, the Department of Defense, and the Department of Justice in February 2016 states that federal agencies should establish procedures for maintaining programs that, among other things:

- facilitate timely sharing of classified cyber threat indicators and defensive measures with representatives of non-federal entities that have appropriate security clearances; and
- share cyber threat indicators, defensive measures, and cyber threat information that may be declassified and shared with non-federal entities at an unclassified level.


Based on the lack of documented coordination responsibilities between HC3 and HTOC, and the need to improve information sharing to the HPH

private-sector partners, we continue to believe that the department should formalize coordination between HC3's and HTOC's information sharing efforts. Doing so would assist with strengthening the HPH sector's private partners' cyber mitigation efforts; it would also align with federal guidance on sharing information with non-federal entities. Accordingly, we believe our recommendation is warranted.

Beyond the aforementioned comments, HHS, DHS CISA, and the Executive Director for Cybersecurity in the HPH Sector Coordinating Council provided technical comments, which we have incorporated in the report, as appropriate.

We are sending copies of this report to appropriate congressional committees, the Secretary of the Department of Health and Human Services, the HHS Chief Information Officer, appropriate officials at the HHS Assistant Secretary for Preparedness and Response, the HHS Inspector General, and other interested parties. This report will also be available at no charge on our website at <http://www.gao.gov>.

If you or your staff have any questions about this report, please contact me at (404) 679-1831 or franksj@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix III.



Jennifer R. Franks
Director, Information Technology and Cybersecurity

List of Requesters

The Honorable Ron Wyden
Chair
Committee on Finance
United States Senate

The Honorable Frank Pallone, Jr.
Chairman
The Honorable Cathy McMorris Rodgers
Republican Leader
Committee on Energy and Commerce
House of Representatives

The Honorable Diana DeGette
Chairwoman
The Honorable H. Morgan Griffith
Republican Leader
Subcommittee on Oversight and Investigations
Committee on Energy and Commerce
House of Representatives

The Honorable Brett Guthrie
House of Representatives

Appendix I: Objectives, Scope, and Methodology

Our specific objectives for this review were to determine the (1) roles and responsibilities that the Department of Health and Human Services (HHS) has defined for its entities to manage cybersecurity within the department; (2) roles and responsibilities that HHS has defined for its entities to assist the cybersecurity efforts of healthcare and public health (HPH) critical infrastructure sector organizations; and (3) extent to which HHS entities have effectively collaborated to manage their cybersecurity responsibilities, including Coronavirus Disease 2019 (COVID-19) cyber response efforts.

To address the first objective, we considered a key principle of an effective control environment on management establishing an organizational structure, assigning responsibility, and delegating authority to achieve the entity's objectives.¹ To determine how HHS determined its roles and responsibilities to meet its internal cybersecurity objectives, we analyzed HHS organizational charts for the full department and the Office of the Chief Information Officer (OCIO); departmental cybersecurity policies and procedures; and strategic and operational plans. In reviewing these documents, we identified the HHS entities (e.g., offices, divisions, and centers) that had been assigned roles for managing cybersecurity within the department.

We also reviewed HHS cybersecurity policies and procedures and strategic and operational plans, and assessed the roles and responsibilities of the entities in comparison to the eight elements of a cybersecurity program, as defined by the Federal Information Security Modernization Act of 2014 (FISMA).² In addition, we interviewed senior officials in HHS OCIO to verify that the HHS entities we identified had significant roles in managing the department's cybersecurity. We also discussed the responsibilities for these officials in fulfilling those roles.

To address the second objective, we considered a key principle of an effective control environment on management establishing an organizational structure, assigning responsibility, and delegating authority

¹GAO, *Standards for Internal Control in the Federal Government*, [GAO-14-704G](#) (Washington, D.C.: Sept. 10, 2014).

²The *Federal Information Security Modernization Act of 2014* (Pub. L. No. 113-283, Dec. 18, 2014) largely superseded the *Federal Information Security Management Act of 2002*, enacted as Title III, *E-Government Act of 2002*, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002).

to achieve the entity's objectives.³ To assess how HHS determined its entities' roles and responsibilities to meet its cybersecurity objectives for the HPH sector, we analyzed organizational charts for the full department, OCIO, the Office of the Assistant Secretary for Preparedness and Response (ASPR), and the Office of the National Coordinator for Health Information Technology; cybersecurity-related policies and procedures; operational and strategic plans; and HPH sector plans. In reviewing these documents, we identified the HHS entities with designated roles for assisting with cybersecurity efforts in the HPH sector.

We also reviewed HHS cybersecurity policies and procedures, strategic and operational plans, and HPH sector plans, and assessed the roles and responsibilities of the entities in comparison to federal requirements related to cybersecurity in the HPH sector, such as those defined by Presidential Policy Directive 21, *Critical Infrastructure Security and Resilience*, the *Cybersecurity Act of 2015*, and the *Health Information Technology for Economic and Clinical Health Act*.⁴ Further, we interviewed senior officials in the HHS OCIO, ASPR, and the Office of the National Coordinator for Health Information Technology to verify that the HHS entities we identified had significant roles in assisting the HPH sector with cybersecurity. We also discussed these officials' responsibilities for fulfilling those roles.

We used the steps recommended by GAO's fragmentation, overlap, and duplication evaluation guide to identify whether there was any fragmentation, overlap, or duplication in the entities we identified with roles in cybersecurity.⁵ More specifically, we analyzed the department's cybersecurity policies and procedures, and strategic and operational plans to:

- identify whether the entities shared similar goals and outcomes;
- determine if clear and distinct roles and responsibilities were defined for the entities;

³[GAO-14-704G](#)

⁴White House, Presidential Policy Directive 21 (PPD 21), *Critical Infrastructure Security and Resilience* (Feb. 12, 2013); the *Cybersecurity Act of 2015* was enacted as part of the *Consolidated Appropriations Act, 2016*, Pub. L. No. 114-113, div. N, § 405, 129 Stat. 2242, 2981 (Dec. 18, 2015); and Pub. L. No. 111-5, Title XIII, 123 Stat. 226,279 (Feb. 17, 2009).

⁵*Fragmentation, Overlap, and Duplication: An Evaluation and Management Guide*, [GAO-15-49SP](#) (Washington, D.C.: Apr. 14, 2015).

- understand the relationship between the entities (i.e., how activities are coordinated, how information is shared, and how activities are jointly planned and implemented);
- determine the effects of any identified fragmentation, overlap, or duplication in the entities' roles and responsibilities; and
- identify the means by which the entities could increase efficiency and reduce or better manage the fragmentation, overlap, or duplication.

To address the third objective, we assessed control activities related to two key internal control principles that management should design control activities to achieve objectives and respond to risks, and implement control activities through policies.⁶ Specifically, we assessed the department's efforts to use collaboration to manage their cybersecurity responsibilities by reviewing relevant documentation on the management and operation of the collaborative groups involved in addressing cybersecurity within the department and HPH sector.

To do this, we identified the groups that the HHS entities told us they use for cybersecurity collaboration within the department and HPH sector. We then selected for review, the seven cybersecurity-focused groups for which the HHS entities maintained operational documentation (i.e., charters and concepts of operation).⁷ These collaborative groups were the:

- HHS Chief Information Security Officer Council
- HHS Cloud Security Working Group
- HHS Continuous Monitoring and Risk Scoring Working Group
- Healthcare Threat Operations Center
- HHS Cybersecurity Working Group

⁶[GAO-14-704G](#).

⁷HHS officials in OCIO's Office of Information Security informed us that there are several working groups chartered under the Chief Information Security Officer Council. Those working groups include the Federal Information Security Modernization Act and Cybersecurity Awareness, Training, and Education working groups. In addition, the six HHS operating divisions that we selected for this review informed us of other cybersecurity-related working groups, such as the HHS Incident Response Team, HHS IT Strategic Workforce, HHS Cybersecurity Workforce Development, Cyber Threat Coordination working groups, and others. However, the officials in the Office of Information Security did not provide charters or other documentation describing the operation of these working groups.

- HPH Sector Government Coordinating Council's Cybersecurity Working Group
- Joint HPH Cyber Working Group

We reviewed charters and concepts of operations for these groups and assessed these documents against seven leading collaboration practices that were identified in our prior work.⁸ Those practices are listed here.

- **Outcomes and accountability** address whether short- and long-term outcomes have been clearly defined, and the extent tracking and monitoring of progress in achieving outcomes has been performed.
- **Bridging organizational cultures** includes identifying the missions and cultures of the participating organizations in the collaborative groups.
- **Leadership** involves designating an individual who will lead the collaborative groups.
- **Clarity of roles and responsibilities** addresses whether the collaborative groups have clarified roles and responsibilities.
- **Participants** includes ensuring that all relevant participants are involved in the collaborative groups.
- **Resources** involves leveraging relevant staff and IT resources to support the operations of the collaborative groups.
- **Written guidance and agreements** includes documenting the collaborative groups' agreement regarding how they will collaborate and determining ways to continually update and monitor these agreements.

To further evaluate the effectiveness of collaboration, we assessed the HHS entities' information sharing processes as they pertain to three key principles of internal control information and communication activities: that management should use quality information to achieve the entity's objectives; internally communicate the necessary quality information to achieve the entity's objectives; and externally communicate the necessary quality information to achieve the entity's objectives.⁹ Specifically, we obtained documentation, such as flow charts and

⁸GAO, *Results-Oriented Government: Practices That Can Help Enhance and Sustain Collaboration among Federal Agencies*, [GAO-06-15](#) (Washington, D.C.: Oct. 21, 2005) and *Managing for Results: Key Considerations for Implementing Interagency Collaborative Mechanisms*, [GAO-12-1022](#) (Washington, D.C.: Sept. 27, 2012).

⁹[GAO-14-704G](#).

standard operating procedures, and interviewed senior HHS officials to identify the processes used by the HHS entities to share cybersecurity information, including cybersecurity-related efforts during COVID-19 response. We then compared the HHS entities' information sharing processes to the internal control standards that recommend management to identify relevant information from reliable sources to make informed decisions and address risks; communicate necessary quality information internally and externally; use appropriate methods of communication for internal and external information sharing.

We supplemented our analyses by interviewing senior officials from the HHS OCIO, ASPR, and Office of the National Coordinator for Health Information Technology. We obtained information on any challenges they had identified in collaborating with relevant sector partners to implement their roles and responsibilities for department and HPH sector cybersecurity.

Further, we interviewed officials charged with leading cybersecurity efforts in six HHS operating divisions to obtain their perspectives on the identified HHS entities' efforts to collaborate to implement their roles and responsibilities for managing the department-wide cybersecurity program. We selected the operating divisions based on the number and type of information systems they operate (i.e., low-, moderate-, and high-impact),¹⁰ as reported in HHS's fiscal year 2019 FISMA report.

Specifically, we ranked the operating divisions by the number of information systems they reported operating during fiscal year 2019. We then separated the operating divisions into categories of large, medium, and small based on the number of systems reported. Within each of these categories, we selected two divisions—one reporting the highest number of high-impact systems and one reporting the highest number of moderate-impact systems. In instances where the operating divisions within the large, medium, and small categories were tied in the highest number of high- and moderate-impact systems, we used a random

¹⁰Information systems are categorized according to the magnitude of harm or impact resulting from the system or its information being compromised. The *Standards for Security Categorization of Federal Information and Information Systems* define three impact levels where the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect (low), a serious adverse effect (moderate), or a severe or catastrophic adverse effect (high) on organizational operations, organizational assets, or individuals. *Federal Information Processing Standards Publication 199, Standards for Security Categorization of Federal Information and Information Systems* (Gaithersburg, Md.: February 2004).

number generator to select between the two operating divisions that were tied. Additionally, if a category of large, medium, and small operating divisions did not have any high-impact systems, we selected the two divisions with the highest number of moderate-impact systems.

The six operating divisions were the

- Food and Drug Administration
- Centers for Medicare and Medicaid Services
- Centers for Disease Control and Prevention
- Health Resource and Services Administration
- Substance Abuse and Mental Health Services Administration
- Agency for Health Research and Quality

In addition, we interviewed the HPH Sector Coordinating Council's Executive Director for Cybersecurity to obtain information on the relevant HHS entities' efforts to collaborate with private sector partners to implement their roles and responsibilities for HPH sector cybersecurity.¹¹ Lastly, we interviewed senior officials at the Department of Homeland Security Cybersecurity and Infrastructure Security Agency to obtain information and documentation on their efforts to coordinate with HHS to share cybersecurity information and resources with the HPH sector.

We conducted this performance audit from November 2019 to June 2021 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.

¹¹Sector Coordinating Councils consist of private organizations and serve as the voice for their respective sector and principal entryway for the government to collaborate with each sector.

Appendix II: Department of Health and Human Services' Cybersecurity-Related Information Sharing Products

The Department of Health and Human Services (HHS) has assigned roles and responsibilities for managing cybersecurity within the department and for assisting with cybersecurity efforts in the healthcare and public health (HPH) critical infrastructure sector. To carry out these activities, the following five HHS entities have shared information to strengthen cybersecurity within the department and HPH sector:

- Office of the Chief Information Officer's Office of Information Security
- Computer Security Incident Response Center
- Health Sector Cybersecurity Coordination Center
- Office of the Assistant Secretary for Preparedness and Response
- Healthcare Threat Operations Center

Table 9 provides a description of the cybersecurity-related information and products that the five entities developed and disseminated to the department's operating and staff divisions and HPH sector. The entities shared these products to provide awareness of ongoing cybersecurity threats and issues, and to assist the operating and staff divisions of the department and organization in the HPH sector with preparing for, and responding to, cyberattacks.

Table 8: Information Sharing Products Used by the Department of Health and Human Services (HHS) Entities to Help Strengthen Cybersecurity within the Department and Healthcare and Public Health (HPH) Critical Infrastructure Sector

HHS entity	Product Type	Description
Office of Information Security	Newsletters	CyberCARE: Provides regular updates on cyber hygiene and best practices to provide awareness of cybersecurity trends, techniques, threats, and vulnerabilities. HHS cybersecurity: Provides cybersecurity threats and vulnerabilities, useful cybersecurity topics, and upcoming cybersecurity events and deadlines. 405(d) post: Shares information intended to broaden awareness and align healthcare industry security approaches.
	Webinars	405(d) spotlight webinar: Highlights cybersecurity issues related to aligning healthcare industry security approaches.
	Posters	405(d) posters: One page graphical products focusing on a single topic or issue, such as tips on telework and cyber safety.
Computer Security Incident Response Center	Cybersecurity notifications	Bulletins: Provides information that is general and informative in nature and may pose or may not pose risks to HHS. Alerts: Includes information that should be addressed immediately on threats or activities that pose, or potentially pose, an impact to the HHS environment. Advisories: Provides information on ongoing cyber events or activity with the potential to impact the department's critical infrastructure computing networks. Traffic notifications: Provides situational awareness regarding suspicious activity observed propagating on HHS and associated operating divisions' networks.

Appendix II: Department of Health and Human Services' Cybersecurity-Related Information Sharing Products

HHS entity	Product Type	Description
Health Sector Cybersecurity Coordination Center ^a	Cybersecurity briefings	Cybersecurity threat intelligence briefings: Provide relevant cybersecurity topics and raise the Healthcare and Public Health sector's situational awareness of current cyber threats, best practices, and mitigation tactics.
	Cybersecurity alerts	Security-related information includes, but is not limited to, new vulnerabilities or malicious actors threatening the healthcare and public health sector that needs immediate attention.
	Cybersecurity white paper	Includes in-depth information on a cybersecurity topic to increase comprehensive situational awareness and provide recommendations to a wide audience.
Office of the Assistant Secretary for Preparedness and Response	Newsletters	Newsletter: Includes cyber threat and other relevant information that it receives from the Health Sector Cybersecurity and Coordination Center and other federal partners.
Healthcare Threat Operations Center ^b	Cyber alert, warning, and threat intelligence	Provides cybersecurity threats and vulnerabilities to strengthen the security and resilience of the federal healthcare partners—HHS, the Department of Veterans Affairs, and the Defense Health Agency.

Source: GAO analysis of information provided by the Department of Health and Human Services. | GAO-21-403

Note: The Office of Information Security distributes the CyberCare and HHS Cybersecurity newsletters internally to the HHS operating and staff divisions, and the 405(d) Post newsletter and posters are distributed to the HPH sector. The Computer Security Incident Response Center sends the cybersecurity reports and notifications throughout the department. The Health Sector Cybersecurity Coordination Center disseminates the cybersecurity briefings, alerts, and white papers across the department and the HPH sector, and the Office of the Assistant Secretary for Preparedness and Response send the newsletters to the HPH sector.

^aAccording to Health Sector Cybersecurity Coordination Center (HC3) Strategic Plan, HC3 is responsible for ensuring that the healthcare and public health sector has the latest threat information, engages in routine and coordinated risk information sharing, protects against advanced persistent threats, and develops proactive risk management strategies.

^bThe Healthcare Threat Operations Center (HTOC) Concept of Operations states that HTOC was established to provide the federal healthcare partners with situational awareness that strengthens the security and resilience of the federal healthcare IT systems, networks, and critical infrastructure.

Appendix III: Comments from the Department of Health and Human Services



DEPARTMENT OF HEALTH & HUMAN SERVICES

OFFICE OF THE SECRETARY

Assistant Secretary for Legislation
Washington, DC 20201

May 26, 2021

Jennifer R. Franks
Director, Information Technology & Cybersecurity
U.S. Government Accountability Office
441 G Street NW
Washington, DC 20548

Dear Ms. Franks:

Attached are comments on the U.S. Government Accountability Office's (GAO) report entitled, "*Cybersecurity: HHS Defined Roles and Responsibilities, but Can Further Improve Collaboration*" (Job code 103878/GAO-21-403).

The Department appreciates the opportunity to review this report prior to publication.

Sincerely,

Rose M.
Sullivan -S

Digitally signed by Rose
M. Sullivan -S
Date: 2021.05.28 12:30:57
-04'00'

Rose Sullivan
Acting Assistant Secretary for Legislation
Principal Deputy Assistant Secretary for Legislation

Attachment

GENERAL COMMENTS FROM THE DEPARTMENT OF HEALTH & HUMAN SERVICES ON THE GOVERNMENT ACCOUNTABILITY OFFICE'S DRAFT REPORT ENTITLED — CYBERSECURITY: HHS DEFINED ROLES AND RESPONSIBILITIES, BUT CAN FURTHER IMPROVE COLLABORATION (GAO-21-403)

The U.S. Department of Health & Human Services (HHS) appreciates the opportunity from the Government Accountability Office (GAO) to review and comment on this draft report.

Recommendation 1

The Secretary of HHS should direct the *Chief Information Officer* to coordinate cybersecurity information sharing between the Health Sector Cybersecurity Coordination Center and Healthcare Threat Operations Center. **(Recommendation 1)**

HHS Response

HHS non-concur with GAO's recommendation.

As discussed throughout the engagement, there exists close coordination between the HTOC and HC3 organizations, mindful of both the stakeholders and agreements between relevant partners and stakeholders. HHS does not believe there exists any duplication of the information disseminated by either entity. With respect to the sharing of HTOC data, due to the high level of fidelity and sensitivity that surround federal intelligence data and the HTOC federal partner cybersecurity operational data, HTOC partners do not share information outside the partnership without the expressed permission and authorization of the originating agency. HTOC reviews intelligence data from sources such as the Department of Homeland Security (DHS), open source data, the HC3 and subscription-based intelligence sources.

Recommendation 2

The Secretary of HHS should direct the *Chief Information Officer* to monitor, evaluate, and report on the progress and performance of the HHS Chief Information Security Officer's Council, Continuous Monitoring and Risk Scoring Working Group, and Cloud Security Working Group. **(Recommendation 2)**

HHS Response

HHS concurs with GAO's recommendation.

HHS CISO Council

Concur. As stated during this engagement, HHS revises charters when the intent or function of the working groups change, or when otherwise deemed necessary. No significant changes have occurred that warrant modifications to the HHS CISO Council charter. Regular monthly meetings also demonstrate the fulfillment of this Council's goals to promote collaboration and information sharing between and among the CISO community. HHS is considering applicable methods to monitor, evaluate, and report on the progress and performance of the HHS CISO Council. Expected outputs and activities of this exercise includes convening a brainstorming session and presenting potential measures to the CISO Council for feedback and adjustments, and to determine if measures and criteria are beneficial to this group. Anticipated timing for completion of this activity is by the end of 2021.

**Appendix III: Comments from the Department
of Health and Human Services**

GENERAL COMMENTS FROM THE DEPARTMENT OF HEALTH & HUMAN SERVICES ON THE GOVERNMENT ACCOUNTABILITY OFFICE'S DRAFT REPORT ENTITLED — CYBERSECURITY: HHS DEFINED ROLES AND RESPONSIBILITIES, BUT CAN FURTHER IMPROVE COLLABORATION (GAO-21-403)

Cloud Security Working Group

Concur. HHS is in the process of updating the Cloud Security Working Group (CSWG) charter and developing performance measures to monitor, evaluate, and report on the progress of this group. The anticipated date for socializing these proposed measures to the OpDivs, and finalizing and obtaining leadership approval and signatures is the end of 2021.

Continuous Monitoring and Risk Scoring Working Group

Concur. HHS is in the process of transitioning the current Continuous Monitoring and Risk Scoring Working Group charter to support the creation of the Information Security Continuous Monitoring Working Group (ISCM WG) to include developing performance measures to monitor, evaluate, and report on the progress of the ISCM WG. HHS anticipates approval by September 2021.

Recommendation 3

The Secretary of HHS should direct the Assistant Secretary for Preparedness and Response to monitor, evaluate, and report on the progress and performance of the Government Coordinating Council's Cybersecurity Working Group and HHS Cybersecurity Working Group. **(Recommendation 3)**

HHS Response

HHS concurs with GAO's recommendations.

ASPR and OCIO are currently co-leading the efforts for the restructuring of the HHS-Cyber working group with the goal of increasing its operational efficiency and cross operating division collaboration. This work will include will include the development of an annual process, to be implemented in calendar year 2022, that has a continuous feedback loop between private sector, USG, and HHS to ensure full coordination on prioritization of activities. This process includes the ability to monitor, evaluate, and report on progress and performance of the Working Groups.

Recommendation 4

The Secretary of HHS should direct the *Chief Information Officer* to regularly monitor and update written agreements describing how the HHS Chief Information Security Officers Council, Continuous Monitoring and Risk Scoring Working Group, and Cloud Security Working Group will facilitate collaboration, and ensure that authorizing officials review and approve the updated agreements. **(Recommendation 4)**

HHS Response

HHS concurs with GAO's recommendations.

HHS CISO Council

Concur. As stated during this engagement, HHS revises charters when the intent or function of the working groups change, or when otherwise deemed necessary. No significant changes have occurred that warrant modifications to the HHS CISO Council charter. Furthermore, regular monthly meetings also demonstrate the fulfillment of this Council's goals to promote collaboration

**Appendix III: Comments from the Department
of Health and Human Services**

GENERAL COMMENTS FROM THE DEPARTMENT OF HEALTH & HUMAN SERVICES ON THE GOVERNMENT ACCOUNTABILITY OFFICE'S DRAFT REPORT ENTITLED — CYBERSECURITY: HHS DEFINED ROLES AND RESPONSIBILITIES, BUT CAN FURTHER IMPROVE COLLABORATION (GAO-21-403)

and information sharing between and among the CISO community. HHS will review the current charter and update as needed. After this review, and any needed updates applied, finalization, approvals, and signatures is anticipated by the end of 2021.

Cloud Security Working Group

Concur. HHS is in the process of updating the Cloud Security Working Group charter. The target timeframe for finalizing and obtaining approvals and signatures is by the end of 2021.

Continuous Monitoring and Risk Scoring Working Group

Concur. There have been significant changes in broadening the scope of this working group to cover Information Security Continuous Monitoring (ISCM). HHS has reviewed the existing charter and resultantly developed a new charter for the ISCM working group that is in a final draft status and submitted for signature. HHS anticipates approval by September 2021.

Recommendation 5

The Secretary of HHS should direct the *Assistant Secretary for Preparedness and Response* to ensure that authorizing officials review and approve the charter describing how the HHS Cybersecurity Working Group will facilitate collaboration. **(Recommendation 5)**

HHS Response

HHS concurs with GAO's recommendations. HHS has met this development and practice.

Recommendation 6

The Secretary of HHS should direct the Assistant Secretary for Preparedness and Response to (1) finalize written agreements that include a description of how the Government Coordinating Council's Cybersecurity Working Group will collaborate, (2) identify the roles and responsibilities of the work group, (3) monitor and update the written agreements on a regular basis, and (4) ensure that authorizing officials leading the working group approve the finalized agreements.

HHS Response

HHS concurs with GAO's recommendations.

ASPR and OCIO are currently co-leading the revise of the CWG charter and the development of a detailed RACI matrix to frame a clear map of roles and responsibilities among stakeholders. This work is expected to be completed by September 2021 at which time, it will be presented to HHS senior leadership for approval. Once completed, ASPR will use the new HHS-CWG charter and RACI chart as a framework for the restructuring of GCC-CWG (expected completion date of Dec 2021).

Recommendation 7

The Secretary of HHS should direct the Assistant Secretary for Preparedness and Response to update the charter for the Joint Healthcare and Public Health Cybersecurity Working Group for

**Appendix III: Comments from the Department
of Health and Human Services**

**GENERAL COMMENTS FROM THE DEPARTMENT OF HEALTH & HUMAN
SERVICES ON THE GOVERNMENT ACCOUNTABILITY OFFICE'S DRAFT
REPORT ENTITLED — CYBERSECURITY: HHS DEFINED ROLES AND
RESPONSIBILITIES, BUT CAN FURTHER IMPROVE COLLABORATION
(GAO-21-403)**

the current fiscal year, and ensure that authorizing officials leading the working group review and approve the updated charter.

HHS Response

HHS concurs with GAO's recommendations.

ASPR and OCIO are currently co-leading the revise of the CWG charter. This work is expected to be completed by September 2021 at which time, it will be presented to HHS senior leadership for approval. The charter and priorities of the GCC CWG will be used to update the Joint Healthcare and Public Health Cybersecurity Working Group charter and governance structure by January 2022.

Appendix IV: GAO Contacts and Staff Acknowledgments

GAO Contact

Jennifer R. Franks, (404) 679-1831, franksj@gao.gov.

Staff Acknowledgments

In addition to the individual named above, Vijay D'Souza and Gregory Wilshusen (directors), Kush K. Malhotra (assistant director), Di'Mond Spencer (analyst-in-charge), Christy Abuyan, Chris Businsky, Nancy Glover, Douglas Harris, Jr., Fatima Jahan, Monica Perez-Nelson, and Sarah Veale made key contributions to this report.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its [website](#) newly released reports, testimony, and correspondence. You can also [subscribe](#) to GAO's email updates to receive notification of newly posted products.

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, <https://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on [Facebook](#), [Flickr](#), [Twitter](#), and [YouTube](#).
Subscribe to our [RSS Feeds](#) or [Email Updates](#). Listen to our [Podcasts](#).
Visit GAO on the web at <https://www.gao.gov>.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: <https://www.gao.gov/about/what-gao-does/fraudnet>

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

Orice Williams Brown, Managing Director, WilliamsO@gao.gov, (202) 512-4400,
U.S. Government Accountability Office, 441 G Street NW, Room 7125,
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

Stephen J. Sanford, Acting Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548

