United States Government Accountability Office

Report to Congressional Committees

December 2023

MEDICAL DEVICE CYBERSECURITY

Agencies Need to Update Agreement to Ensure Effective Coordination

GAO-24-106683

GAO Highlights

Highlights of GAO-24-106683, a report to congressional committees

December 2023

MEDICAL DEVICE CYBERSECURITY

Agencies Need to Update Agreement to Ensure Effective Coordination

Why GAO Did This Study

Cyber threats that target medical devices could delay critical patient care, reveal sensitive patient data, shut down health care operations, and necessitate costly recovery efforts. FDA is responsible for ensuring that medical devices sold in the U.S. provide reasonable assurance of safety and effectiveness.

The Consolidated Appropriations Act, 2023, includes a provision for GAO to review cybersecurity in medical devices. This report addresses the extent to which (1) relevant non-federal entities are facing challenges in accessing federal support on medical device cybersecurity, (2) federal agencies have addressed identified challenges, (3) key agencies are coordinating on medical device cybersecurity, and (4) limitations exist in agencies' authority over medical device cybersecurity.

GAO identified federal agencies with roles in medical device cybersecurity. It also selected 25 non-federal entities representing health care providers, patients, and medical device manufacturers. GAO interviewed these entities on challenges in accessing federal cybersecurity support. In addition, GAO assessed agency documentation and compared coordination efforts against leading collaboration practices; reviewed relevant legislation and guidance; and interviewed agency officials.

What GAO Recommends

GAO is making recommendations to FDA and CISA to update their agreement to reflect organizational and procedural changes that have occurred. Both agencies concurred with the recommendations.

View GAO-24-106683. For more information, contact Jennifer R. Franks at (404) 679-1831 or franksj@gao.gov

What GAO Found

According to the Department of Health and Human Services (HHS), available data on cybersecurity incidents in hospitals do not show that medical device vulnerabilities have been common exploits. Nevertheless, HHS maintains that such devices are a source of cybersecurity concern warranting significant attention and can introduce threats to hospital cybersecurity (see figure).

Figure: Example of a Compromised Medical Device That Can Lead to Disruption of Other Devices on a Hospital Network

1. Threat actor gains access to a healthcare provider's network by exploiting a vulnerability (e.g. a phishing attack).
2. Threat actor takes command of a server to which a patient heart monitor is attached.
3. While scanning the network, the threat actor takes control of all heart monitors and is able to shut them off, which puts additional patients at risk.
4. Threat actor could compromise other devices on the network, adding to patient risk.

Sources: GAO interpretation of Department of Health and Human Services example (illustrations); gofficon/stock.adobe.com (icons); elenabsl/stock.adobe.com (illustrations). | GAO-24-106683

Non-federal entities representing health care providers, patients, and other relevant parties identified challenges in accessing federal support to address cybersecurity vulnerabilities. Entities described challenges with (1) a lack of awareness of resources or contacts and (2) difficulties understanding vulnerability communications from the federal government. Agencies are taking steps that, if implemented effectively, can meet these challenges.

Key agencies are also managing medical device cybersecurity through active coordination. Specifically, the Food and Drug Administration (FDA) and the Cybersecurity and Infrastructure Security Agency (CISA) developed an agreement addressing most leading practices for collaboration. However, this 5-year-old agreement did not address all such practices and needs to be updated to reflect organizational and procedural changes that have occurred since 2018.

FDA authority over medical device cybersecurity has recently increased. Specifically, December 2022 legislation requires medical device manufacturers to submit to FDA, among other things, their plans to monitor, identify, and address cybersecurity vulnerabilities for any new medical device that is to be introduced to consumers starting in March 2023. This legislation is limited to new devices and does not retroactively apply to those devices introduced prior to March 2023, unless the manufacturer is submitting a new marketing application for changes to the device.

FDA officials are implementing new cybersecurity authorities and have not yet identified the need for any additional authority. They can take measures to help ensure device cybersecurity under existing authorities such as monitoring health sector and CISA alerts, as well as directing manufacturers to communicate vulnerabilities to user communities and to remediate the vulnerabilities.

According to FDA guidance, if manufacturers do not remediate vulnerabilities, FDA may find the device to be in violation of federal law and subject to enforcement actions.

Contents

Figure

Abbreviations

ASPR	Administration for Strategic Preparedness and Response
CISA	Cybersecurity and Infrastructure Security Agency
EHR	Electronic Health Record
FBI	Federal Bureau of Investigation
FDA	Food and Drug Administration
HHS	Department of Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act of 1996
HSCC	Healthcare and Public Health Sector Coordinating Council
IT	information technology
MRI	magnetic resonance imaging
NIST	National Institute of Standards and Technology
OCR	Office for Civil Rights
PHI	protected health information
VA	Department of Veterans Affairs

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

December 21, 2023

The Honorable Bernard Sanders
Chair
The Honorable Bill Cassidy
Ranking Member
Committee on Health, Education, Labor and Pensions
United States Senate

The Honorable Cathy McMorris Rodgers
Chair
The Honorable Frank Pallone, Jr.
Ranking Member
Committee on Energy and Commerce
House of Representatives

With the increasing integration of wireless, internet- and network-connected capabilities, and the electronic exchange of health information, the need for robust cybersecurity controls to ensure medical device safety and effectiveness is increasingly important. In addition, cybersecurity threats to the healthcare sector have become more frequent and more severe, carrying increased potential for impact in clinical settings.

According to a study by the Department of Health and Human Services (HHS) and the Healthcare and Public Health Sector Coordinating Council (HSCC), medical devices have not typically been exploited to disrupt clinical operations in hospitals. However, the study states that they are a source of cybersecurity concern warranting significant attention.[1] Specifically, device vulnerabilities can allow advanced forms of cyber

[1]Department of Health and Human Services and Healthcare & Public Health Sector Coordinating Council, *Hospital Cyber Resiliency Initiative: Landscape Analysis* (Washington, D.C.: Apr. 2023). The Healthcare & Public Health Sector Coordinating Council is a chartered organization comprised of private sector entities with equities in or closely aligned to the Healthcare and Public Health Sector. The sector coordinating council is recognized by the Secretary of Health and Human Services as the critical infrastructure industry partner with the government under *Presidential Policy Directive 21.* Their role is to coordinate strategic and policy approaches to mitigating, preparing for, responding to, and recovering from significant cybersecurity and physical threats to the Healthcare and Public Health Sector.

incidents to spread across organizations, and unsupported, legacy medical devices may be considered more vulnerable to cyber incidents.[2]

The Consolidated Appropriations Act, 2023, includes a provision for us to review medical device cybersecurity.[3] This report addresses the extent to which (1) relevant non-federal entities are facing challenges in accessing federal support on medical device cybersecurity, (2) federal agencies have addressed identified challenges, (3) key agencies are coordinating on medical device cybersecurity, and (4) limitations exist in agencies' authority over medical device cybersecurity.

To address our first objective, we selected a set of non-federal entities by reviewing a list of members in the HSCC and focusing on large associations of medical device manufacturers, health systems, and healthcare providers whose missions support medical device cybersecurity. We sought the input of these associations regarding additional entities that had a role or insights on the topic. We also contacted the federal agencies in the scope of our review (described below), as well as GAO subject matter experts, regarding selection of patient advocacy organizations. This resulted in a list of 25 non-federal entities comprised of a cross-section of organizations and experts that represent medical device manufacturers, health systems, health care providers, and patients. We interviewed representatives from these 25 entities and performed an analysis of the interview results to develop a list of challenges.

To address our second and third objectives, we selected a set of agencies with responsibility for medical device cybersecurity. We did so based on a review of previous GAO work and public reports by federal agencies. We also relied on suggestions from officials with the Food and Drug Administration (FDA) and Cybersecurity and Infrastructure Security Agency (CISA). Specifically, we selected the following 11 agencies:

- National Institute of Standards and Technology at the Department of Commerce,
- Defense Health Agency at the Department of Defense,

[2]According to the International Medical Device Regulators Forum, a legacy device is a device that cannot be reasonably protected against current cybersecurity threats.

[3]Pub. L. No. 117-328, § 3305(g), 136 Stat. 4459, 5834 (2022), which amends the Federal Food, Drug, and Cosmetic Act, 21 U.S.C. 351 et. seq.

- Administration for Strategic Preparedness and Response at the Department of Health and Human Services,
- Centers for Medicare and Medicaid Services at the Department of Health and Human Services,
- Food and Drug Administration at the Department of Health and Human Services,
- Indian Health Service at the Department of Health and Human Services,
- Office for Civil Rights at the Department of Health and Human Services,
- Office of the National Coordinator for Health Information Technology at the Department of Health and Human Services,
- Cybersecurity and Infrastructure Security Agency at the Department of Homeland Security,
- Federal Bureau of Investigation at the Department of Justice, and
- Veterans Health Administration at the Department of Veterans Affairs.

We reviewed agency documentation on medical device cybersecurity, as well as any memorandums of agreement or understanding that coordinating agencies had developed.[4] We assessed agency documentation against eight leading collaboration practices[5] and fragmentation, overlap, and duplication from prior GAO work.[6] We also interviewed agency officials with responsibility for medical device cybersecurity, and assessed responses against the leading practices.

To address our fourth objective, we evaluated relevant sections of legislation, regulations, and guidance to understand the scope of agencies' authority over the cybersecurity of medical devices. Specifically, we evaluated relevant portions of the following:

[4]A memorandum of agreement, or memorandum of understanding, is a document describing a partnership between two or more parties that have agreed to cooperate to meet an agreed objective or complete a project.

[5]GAO, *Government Performance Management: Leading Practices to Enhance Interagency Collaboration and Address Crosscutting Challenges*, GAO-23-105520 (Washington, D.C.: May 24, 2023).

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

- Federal Food, Drug, and Cosmetic Act,
- Consolidated Appropriations Act, 2023,
- Health Insurance Portability and Accountability Act (HIPAA) and the HIPAA Security Rule,[7] and
- Federal agency guidance about medical device cybersecurity, including FDA's draft premarket cybersecurity guidance.[8]

Where agencies identified actions to mitigate risk associated with potential limitations, we reviewed documentation associated with FDA's postmarket guidance and coordination with other agencies.[9] We also interviewed agency officials with responsibility over medical device cybersecurity. Appendix I includes additional details on our scope and methodology, and appendix II includes a list of the non-federal entities that we interviewed.

We conducted this performance audit from March 2023 to December 2023 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

The Federal Food, Drug, and Cosmetic Act defines a medical device as an instrument, machine, contrivance, implant, in vitro reagent or a similar or related article that is intended to treat, cure, prevent, mitigate, or diagnose disease. Medical devices range from simple tongue depressors and bedpans to complex programmable pacemakers and closed loop artificial pancreas systems. Recently enacted legislation defines a cyber device as a device that includes software, has the ability to connect to the internet, and is vulnerable to cybersecurity threats.[10]

[7]Pub. L. No. 104-191 Title II, Subtitle F, 110 Stat. 1936, 2021 (Aug. 21, 1996) (codified at 42 U.S.C. §§ 1320d–1320d-9), and the HIPAA Security Rule, 45 C.F.R. Part 164 Subpart C.

[8]87 Fed. Reg. 20873.

[9]Postmarket refers to the time period after introduction of a device into the market for patient and provider use.

[10]21 U.S.C. § 321(h); Consolidated Appropriations Act, 2023, Pub. L. No. 117-328, § 3305(a), 136 Stat. at 5834 (2022)(to be codified at 21 U.S.C. § 360n-2).

Network-Connected Medical Devices Are Vulnerable to Cyber Threats

Cyber incidents that impact medical devices could delay critical patient care, reveal sensitive patient data, shut down health care provider operations, and necessitate costly recovery efforts. According to HHS and HSCC, cyber incidents affecting network-connected medical devices are one of the types of current cyber threats in the Healthcare and Public Health Sector. As devices become more integrated with medicine and more digitally interconnected, securing medical devices against cyber threats is imperative.

Although cyber incidents impacting medical devices have occurred, they are not common. For example, in 2017, investigations by an information risk management and compliance company found that a ransomware attack had impacted medical devices from at least two medical device manufacturers.[11] However, more recently, in 2023, HHS stated that available data on cybersecurity incidents in hospitals do not appear to show that medical device vulnerabilities fall in the category of the most-common exploit vectors.[12] Nevertheless, HHS and HSCC add that disruption to such devices has significant safety and operational impacts.

Many medical devices are network-connected because this can increase efficiency and patient safety in the health industry. Network connected devices allow doctors, nurses, and caretakers to monitor patients' status in real time from one location, and transfer information to electronic health records (EHRs). For example, a patient heart monitor, insulin pump, or blood glucose monitor may be connected to a network via wireless connection or Bluetooth connection to facilitate ease of care.

However, network connections create more avenues for a bad actor, and threats can be spread to and from other devices and systems on the network. Many medical devices are connected to hospital networks, including magnetic resonance imaging (MRI) machines, devices used for telemetry, and many others.[13] Because threats can be transferred over the hospital network, an infected medical device could allow cyber threats to spread to other devices. Further, these threats could also negatively

[11]Sean Martin, HITRUST Alliance, "WannaCry Post Mortem: Early Warning Indicators and Lessons Learned for the Healthcare Industry" (Aug. 4, 2017), accessed Nov. 8, 2023. https://hitrustalliance.net/wannacry-post-mortem-early-warning-indicators-lessons-learned-healthcare-industry/

[12]Department of Health and Human Services, *Hospital Resiliency Initiative Landscape Analysis* (Washington, D.C.: Apr. 17, 2023).

[13]Telemetry refers to the process of continuously measuring and monitoring a patient's vital signs remotely using medical equipment.

impact the entire hospital network, with potential catastrophic impact to hospital operations and patient care. Threats faced by medical devices can include malware, ransomware, and denial of service, among others.[14]

The Federal Bureau of Investigation (FBI) issued a notification in September 2022 that highlighted the pervasiveness of the cybersecurity threats that medical devices face.[15] For example:

- As of January 2022, 53 percent of connected medical devices and other internet of things devices in hospitals had known critical vulnerabilities.[16] Approximately one third of health care internet of things devices had an identified critical risk, potentially impacting operation and function of the devices.
- Medical devices that are susceptible to cyberattacks include insulin pumps, intracardiac defibrillators, mobile cardiac telemetry, pacemakers, and intrathecal pain pumps. Bad actors who compromise these devices could direct them to give inaccurate readings, administer drug overdoses, or otherwise endanger patient health.
- There is an average of 6.2 vulnerabilities per medical device, and recalls were issued for critical devices such as pacemakers and insulin pumps with known security issues.

Medical devices face known vulnerabilities. Table 1 identifies examples of vulnerabilities that might impact medical devices, and the risks they present to the devices.

[14]Malware is a program that is inserted into a system with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system, or of otherwise annoying or disrupting the victim. Ransomware is a type of malicious software where attackers encrypt an organization's data and demand payment to restore access. Denial of service is the prevention of authorized access to a system resource or the delaying of system operations and functions.

[15]Federal Bureau of Investigation, *Unpatched and Outdated Medical Devices Provide Cyber Attack Opportunities*, Private Industry Notification 2022912-001 (Washington, D.C.: Sept. 12, 2022).

[16]Internet of things technology refers to devices collecting information, communicating it to a network and, in some cases, completing a task—like unlocking doors using a smartphone application.

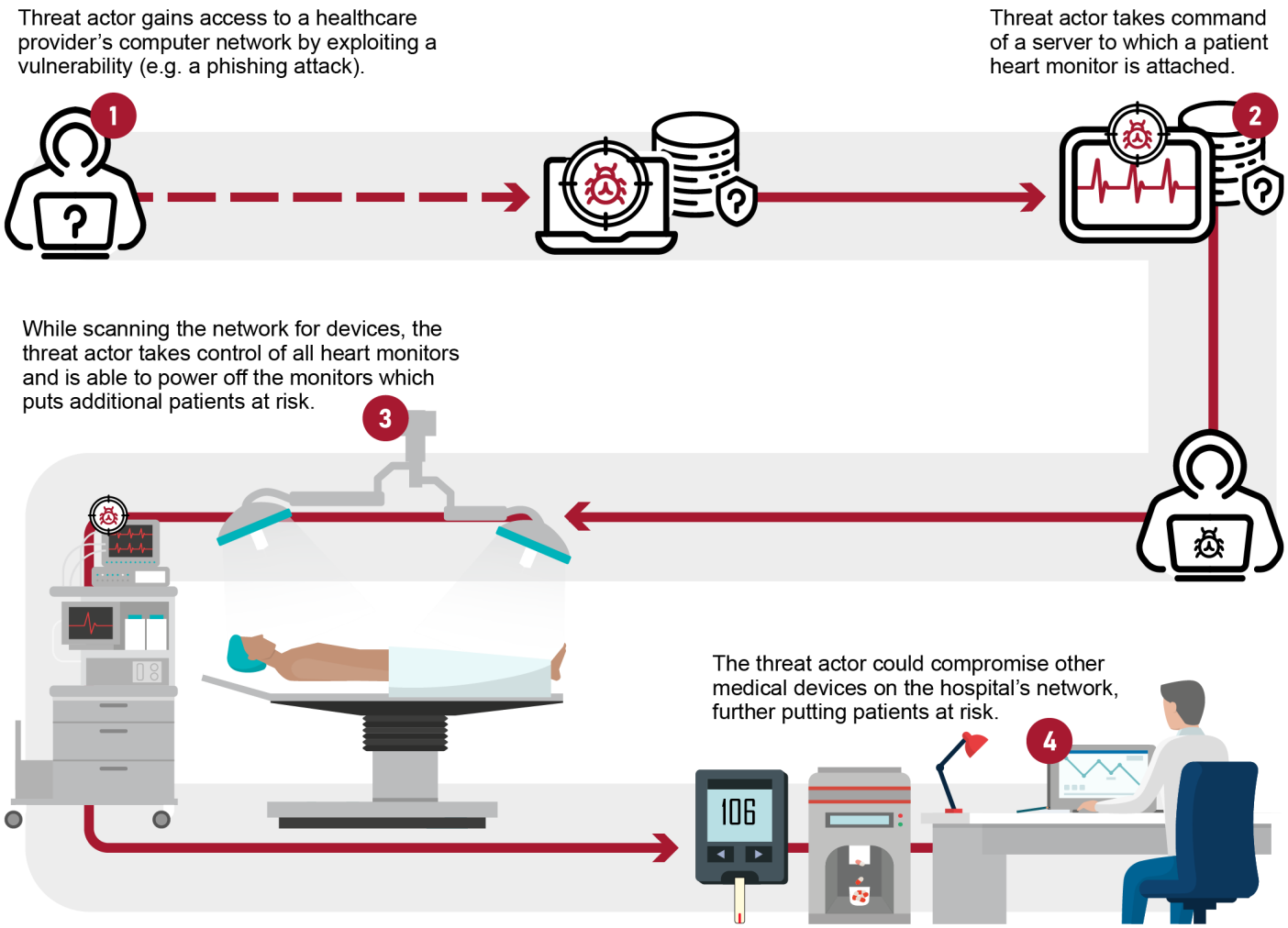
Table 1: Examples of Cybersecurity Vulnerabilities and Associated Risks to Medical Devices

Vulnerability	Risk
Use of insecure default configurations	Medical devices may be delivered to operators or users with certain default configurations that may not be secure by default, like factory settings or manufacturer administrative passwords. If insecure default configurations are maintained, cyber threats may have an avenue to uncover data or inject data, gain privileges, execute commands, etc.
Customized software requiring special upgrading and patching procedures	Because the operators or users of devices may have to rely on a manufacturer's device update processes, there may be a delay in the implementation of vulnerability patching.
Devices without security in design	Medical devices that have been operating for a long time (e.g., decades) may have not been designed with cybersecurity in mind, as they may not have originally been exposed to cybersecurity threats. As such, it may be difficult to secure them in a modern environment.

Source: GAO analysis of Cybersecurity and Infrastructure Security Agency, Department of Health and Human Services, Federal Bureau of Investigation, and Healthcare and Public Health Sector Coordinating Council publications | GAO-24-106683

Figure 1 presents one of many possible scenarios that leverage a medical device as a vector to disrupt hospital operations.

Figure 1: Example of a Compromised Medical Device That Can Lead to Disruption of Other Devices on a Hospital Network



Sources: GAO interpretation of Department of Health and Human Services example (illustrations); gofficon/stock.adobe.com (icons); elenabsl/stock.adobe.com (illustrations). | GAO-24-106683

Legacy Devices Increase the Threat Landscape

The International Medical Device Regulators Forum defines a legacy device as a medical device that cannot be reasonably protected against current cybersecurity threats. This could be because of, for example, device design or lack of maintenance for cybersecurity.[17] For example, an MRI machine may have been in use for multiple decades, and although the machine still functions in a clinical setting, cybersecurity support may not be available due to the device's age. Because legacy devices cannot be reasonably protected, they can be more vulnerable than other devices, which increases risk to the hospital network and other devices on the same network.

Further, the HSCC has stated that the understanding of shared responsibility for maintaining security between medical device manufacturers and health care delivery organizations remains uneven. As such, HSCC recommends that health care delivery organizations, medical device manufacturers, and other health care stakeholders work together to evaluate potential legacy technologies and apply best practices for securing them.

Federal Law Establishes Requirements for Medical Device Cybersecurity

While federal law has addressed medical device safety for decades, cybersecurity in medical devices is a more recent topic. Long-standing federal law, as well as more recent legislation, includes the following:

Federal Food, Drug, and Cosmetic Act.[18] The act, as amended, authorizes FDA to oversee and regulate the production, sale, and distribution of food, drugs, medical devices, and cosmetics. FDA is responsible for ensuring that medical devices sold in the United States provide reasonable assurance of safety and effectiveness and do not pose a threat to public health.[19] This includes ensuring cybersecurity risks do not affect medical device safety and effectiveness.

To assess whether medical devices provide such assurance, FDA conducts a premarket review of medical devices and relies on the sponsor of a device to provide data that supports the device's safety and

[17]The International Medical Device Regulators Forum is a group of medical device regulators from around the world that have voluntarily come together to harmonize the regulatory requirements for medical products that vary from country to country. The Food and Drug Administration represents the United States in the International Medical Device Regulators Forum.

[18]Pub. L. No. 75-717, 52 Stat. 1040 (1938) (codified as amended at 21 U.S.C. §§ 321-399i).

[19]See, e.g., 21 U.S.C. § 360c.

effectiveness. FDA may thereafter request additional data during the review to obtain sufficient evidence supporting the safety and effectiveness of the medical device.[20] The act also provides FDA with the authority to conduct what is known as postmarket surveillance, in which the agency monitors information sources including internal agency information such as recalls, sector risk management alerts, and communication with manufacturers.[21] With respect to cybersecurity, FDA has issued guidance addressing premarket expectations for medical device cybersecurity.[22]

Recent amendments to the Federal Food, Drug, and Cosmetic Act give FDA additional authority over cybersecurity of medical devices.[23] Among other things, the amendments define a cyber device and includes requirements for device manufacturers to:

- have plans to monitor, identify, and address, as appropriate, cybersecurity vulnerabilities and exploits;
- design, develop, and maintain processes and procedures to provide a reasonable assurance that the device and related systems are cyber secure; and
- provide the Secretary of Health and Human Services with a software bill of materials.[24]

[20]FDA classifies each medical device type into one of three classes based on the level of risk it poses to the patient or the user and the controls necessary to reasonably ensure its safety and effectiveness. Class III devices require FDA's premarket approval, the most stringent type of premarket review, and must submit an application that includes full reports of investigations, including clinical data. Class I and class II devices require premarket notification, known as the 510(k) process, although most class I and some class II devices are exempt from the 510(k) process.

[21]Premarket refers to the time period preceding introduction of a device to the market for patient and provider use. Postmarket refers to the time period after a device has been introduced to the market for patient and provider use.

[22]See, for example: Food and Drug Administration, *Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions, Guidance for Industry and Food and Drug Administration Staff* (Silver Spring, MD: Sept. 27, 2023).

[23]Pub. L. No. 117-328, § 3305, 136 Stat. at 5832 (2022).

[24]A software bill of materials is an inventory of the different pieces that make up software components.

Health Insurance Portability and Accountability Act of 1996 (HIPAA).[25] The act authorized the Secretary of HHS to establish standards to protect the privacy of certain health information and required the Secretary to adopt security standards for that health information. HHS implemented the HIPAA provisions through its issuance of the Privacy, Security, and Breach Rules. The HIPAA Privacy Rule establishes national standards for safeguarding protected health information (PHI), which includes most individually identifiable health information transmitted or maintained in any form by a covered entity or its business associates.[26]

The HIPAA Security Rule establishes nationwide standards for safeguarding protected health information that is held or transmitted electronically. The rule operationalizes the protections contained in the Privacy Rule by specifying administrative, physical, and technical safeguards to secure individuals' electronic PHI. For example, the Security Rule requires organizations to complete a risk analysis that is an accurate and thorough assessment of the potential risks and vulnerabilities to the electronic PHI held by the covered entity or business associate. The Security Rule also requires covered entities and business associates to implement risk management practices such as implementing sufficient security measures to reduce potential risks and vulnerabilities to a reasonable and appropriate level.[27]

The Breach Notification Rule requires covered entities to notify HHS of breaches of unsecured PHI.[28] To comply with this breach notification requirement, covered entities notify HHS of breaches through a reporting system on HHS's breach portal. For breaches that affected 500 or more individuals, covered entities must submit a notification to HHS within 60

[25]Pub. L. No. 104-191, Title II, Subtitle F, 110 Stat. 1936, 2021 (Aug. 21, 1996) (codified at 42 U.S.C. §§ 1320d–1320d-9) and the HIPAA Security Rule, 45 C.F.R. Part 164.

[26]Covered entities include health plans, health care clearinghouses, and health care providers that transmit any health information in electronic form in connection with a transaction for which HHS has adopted standards. A business associate is generally an entity that creates, receives, maintains, or transmits protected health information on behalf of a covered entity for a covered function or performs certain services to or for a covered entity that involve the use or disclosure of PHI.

[27]The Department of Health and Human Service Office for Civil Rights (OCR) is responsible for enforcing the HIPAA Privacy, Security, and Breach Rules. OCR investigates complaints, conducts compliance reviews, and performs education and outreach to foster compliance. Failure to comply with HIPAA can result in civil and criminal penalties.

[28]45 CFR Part 164 Subpart D.

days after the discovery of a breach, and for breaches affecting fewer than 500 individuals, covered entities must notify HHS within 60 days after the end of the calendar year in which the breach occurred.

Federal Agencies and Industry Experts Have Roles in Medical Device Cybersecurity

A variety of federal agencies and other industry groups support cybersecurity in medical devices. Key organizations include the following:

FDA. As described previously, ensuring the safety and effectiveness of medical devices is the responsibility of the FDA—an agency within HHS. The goal of FDA's Center for Devices and Radiological Health is to ensure that patients and providers have timely and continued access to safe, effective, and high-quality medical devices and safe radiation-emitting products. FDA has also published guidance for manufacturers to use as they develop medical devices with the intent of securing those devices.[29]

Other HHS Entities. As the lead agency responsible for managing risks in the Healthcare and Public Health sector, several HHS entities are involved in ensuring cybersecurity in medical devices.[30] For example:[31]

- **The Administration for Strategic Preparedness and Response (ASPR)** leads the nation's medical and public health preparedness for, response to, and recovery from disasters and public health emergencies. Although medical devices are not a specific focus of the administration, they are a subset of the administration's responsibility. ASPR coordinates HHS cybersecurity support and leads external collaboration on behalf of HHS for the Healthcare and Public Health Sector.
- **The Centers for Medicare and Medicaid Services** participates in an FDA-led working group focused on legacy devices. The agency has collaborated with public and private entities to support guidance published by the FDA on securing legacy medical devices.

[29]See, for example: Food and Drug Administration, *Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions, Guidance for Industry and Food and Drug Administration Staff* (Silver Spring, MD: Sept. 27, 2023).

[30]Each of the 16 critical infrastructure sectors has unique characteristics, operating models, and risk profiles. As such, each sector has a designated risk management agency to, among other things, provide, support, or facilitate technical assistance within the sector.

[31]HHS supports a variety of other working groups, as outlined below.

- **The Office for Civil Rights (OCR)** enforces the compliance of HIPAA-regulated entities with the standards and implementation specifications required by the HIPAA Security Rule, as described above.[32] As such, when a HIPAA-regulated entity employs a medical device, any protected health information created, maintained, or transmitted by the device is subject to protections under HIPAA.
- **The Office for the National Coordinator for Health IT** is the principle federal entity charged with coordination of nationwide efforts to implement and use health IT and the electronic exchange of information. Although it plays a coordinating role, the office often defers to FDA for medical device-related matters.
- **The Indian Health Service** is responsible for providing direct medical and public health services to members of federally recognized Native American Tribes and Alaska Native People. As such, the service is responsible for medical devices that are used in clinical settings at federal facilities.

CISA. The agency releases public alerts and advisories that include information about current cybersecurity issues, vulnerabilities, and exploits. CISA specifically publishes industrial control medical advisories for those issues that impact medical devices.[33] CISA has also produced guidance for manufacturers and others to better secure their systems or devices, evaluate the risk, and develop remediation actions.[34]

FBI. The bureau monitors threats in the Healthcare and Public Health Sector. Upon detection of a threat, FBI may inform affected hospitals and

[32]A HIPAA-covered entity or business associate is collectively referred to as a "HIPAA-regulated entity" throughout this report.

[33]An industrial control system is used to control industrial processes such as manufacturing, product handling, production, and distribution. See the following as an example: Cybersecurity and Infrastructure Security Agency, *Industrial Control Medical Advisory 23-117-01* (Arlington, VA: Apr. 27, 2023).

[34]See, for example: Cybersecurity and Infrastructure Security Agency, *CISA Resources Applicable to Threats Against Healthcare & Public Health Sector* (Arlington, VA). CISA has also worked with the Department of Health and Human Services and HSCC to develop a toolkit intended to consolidate key resources for improving cybersecurity in the Healthcare and Public Health sector, which it has published on its website.

health care providers.[35] In addition, it may provide support to affected systems or providers in remediating the effects of cybersecurity incidents.

National Institute of Standards and Technology (NIST). NIST is a non-regulatory and non-oversight agency. With input from the government, academia, and the health care industry, it develops and releases standards, guidance, and frameworks for the health care industry to improve their cybersecurity ecosystem. For example, NIST has published guidance specific to securing the telehealth remote patient monitoring ecosystem under its 1800-series of publications.[36]

Defense Health Agency. This joint, integrated combat support agency enables the Army, Navy, and Air Force medical services to provide a medically ready force to combatant commands in both peacetime and wartime. The agency publishes guidance for, and interacts with, medical device vendors to ensure that they understand the requirements for connecting to Department of Defense resources.[37]

Veterans Health Administration. Within the Department of Veterans Affairs (VA), the Veterans Health Administration is the nation's largest integrated health care system serving around nine million enrolled veterans each year. Both VA and the Veterans Health Administration are responsible for the security of medical devices on agency networks and have developed policy and guidance that medical device manufacturers need to comply with when submitting bids related to VA procurements.[38]

Public-Private Working Groups and Resources. A variety of working groups and resources combine public and private experts to support

[35]For example, see: Federal Bureau of Investigation, *Unpatched and Outdated Medical Devices Provide Cyber Attack Opportunities*, Private Industry Notification 2022912-001 (Washington, D.C.: Sept. 12, 2022).

[36]National Institute of Standards and Technology, *Securing Telehealth Remote Patient Monitoring Ecosystem,* Special Publication 1800-30 (Gaithersburg, MD: Feb. 2022).

[37]See, for example: Defense Health Agency, *Procedural Instruction: Cybersecurity Logistics (CyberLOG) Medical Devices and Equipment (MDE) Risk Management Framework (RMF)* (Mar. 2, 2020).

[38]See, for example: Department of Veterans Affairs, *VA Handbook 6550—Pre-Procurement Assessment and Implementation of Medical Devices/Systems* (Washington, D.C.: June 3, 2019); *VA Handbook 6500.6 – Contract Security* (Washington, D.C.: Mar. 12, 2010).

cybersecurity in medical devices. Government, industry, and health care practitioners collaborate in the following manner:

- **The HHS Joint Cybersecurity Working Group** provides a forum for discussion of cybersecurity issues to improve the security and resilience of Healthcare and Public Health sector information systems and serve as the main body of HHS representatives for cybersecurity expertise for policy issues. The HSCC is a public-private component of this working group.

  In addition, the HSCC's Cyber Working Group is recognized by HHS as the critical infrastructure industry partner with the government for coordinating strategic, policy, and operational approaches to prepare for, respond to, and recover from significant cyber and physical threats to the sector. The working group is composed of hundreds of private entities, and 18 government organizations.[39]
- **The Health Sector Cybersecurity Coordination Center** was created by HHS to aid in the protection of vital, health care-related controlled information and ensure that cybersecurity information sharing is coordinated across the Healthcare and Public Health Sector. The center produces threat briefs that highlight relevant cybersecurity topics and raise the sector's situational awareness of cyber threats, threat actors, best practices, and mitigation tactics. It also provides high-level, situational background information and context for technical and non-technical audiences and provides quick information and in-depth analyses which increase cybersecurity situational awareness.
- **The 405(d) Health Industry Cybersecurity Practices Task Group** attempts to raise awareness and strengthen the Healthcare and Public Health Sector's cybersecurity.[40] This is a collaborative effort between industry and the federal government to develop consensus-based practices and guidelines. 405(d) offers implementation guidance for health care organizations to secure medical devices.[41]

[39]Private entities include, for example, health systems, hospitals, and associations that represent medical device manufacturers, health care providers, and physicians.

[40]The 405(d) Program is an organizational component of HHS, within the Office of the Chief Information Officer. The public-private component of this work is the 405(d) Health Industry Cybersecurity Practices Task Group, which is one of multiple task groups. Additional task groups include, for example, MedTech Joint Security Plan, MedTech Legacy Cybersecurity, and MedTech Vulnerability Communications.

[41]See, for example: 405(d) Program, *Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients* (Washington, D.C.).

- **The Health Information Sharing and Analysis Center** is a global non-profit offering a forum for coordinating, collaborating, and sharing physical and cyber threat intelligence across its members. Membership includes critical infrastructure owners and operators within the Healthcare and Public Health Sector. The organization is primarily focused on sharing timely, actionable, and relevant information with each other.
- **Healthcare and Public Health Sector Risk Management Agency Cyber Working Group's** vision is to coordinate Healthcare and Public Health Sector cybersecurity activities effectively and efficiently across HHS to help protect America's health care and public health infrastructure from emerging and ongoing cyber threats. Membership includes, for example, the Administration for Strategic Preparedness and Response, the Center for Medicare and Medicaid Services, FDA, the Indian Health Service, OCR, and the Office of the National Coordinator for Health IT.

Health Systems, Providers, and Patients Have Identified Challenges in Accessing Federal Support

Federal agencies have made resources available to support non-federal entities in managing cybersecurity vulnerabilities that threaten medical devices. Some, but not all, of non-federal entities identified challenges in accessing federal support to address cybersecurity vulnerabilities that threaten medical devices. Specifically, although six of the medical device manufacturers did not identify challenges, 14 of the remaining 19 entities did. These 19 entities representing health systems, healthcare providers, and patients identified challenges in accessing federal support.[42] The most frequently identified challenges were the following:

Problems understanding vulnerability communications from federal agencies. Eight of the 14 non-federal entities indicated that they or their membership can have problems understanding vulnerability communications from federal entities. For example:

- An alert may be too difficult for users to understand.
- Alerts can sometimes be overwhelming due to the number of notification emails that are received.

[42]In addition to challenges related to accessing federal support, selected non-federal entities also reported other kinds of challenges. For example, entities reported that the regulatory environment concerning medical device cybersecurity is complicated, which can make securing devices more difficult in certain cases. In addition, entities reported challenges in working with medical device vendors. For example, entities reported that vendors may require payment for cybersecurity protections on medical devices such as encryption or antivirus.

- Vulnerability notifications from the government may not be useful to recipients.
- Published federal guidance on cybersecurity vulnerabilities may not be useful.

Lack of awareness of federal contacts or resources. After the discovery of a cybersecurity incident or vulnerability, six non-federal entities stated that they or their membership did not always know who in the federal government to contact, or what resources federal agencies had made available. For example:

- Small or mid-sized hospital systems indicated they may not have direct contact with federal subject matter experts that larger entities might have.
- Entities may be unaware of which federal agency to contact in the event of an incident.
- Entities may not know what resources federal agencies have that can help with cybersecurity awareness.

Agencies Had Generally Taken Actions to Address Identified Challenges

FDA is the primary agency with responsibility over medical device cybersecurity and has employed procedures that can address the identified challenges. Other agencies are also taking actions that, if implemented effectively, should mitigate the challenges.[43] For example:

Agency actions to improve understanding of vulnerability communications. Agencies reported actions they're taking to address the challenge associated with the difficulty in understanding vulnerability communications. For example, the

- FDA has developed resources for vulnerability communications to patients[44] and supported the Healthcare and Public Health Sector Coordinating Council's Cybersecurity Working Group in their development of a communications toolkit.[45] These resources emphasize using, for example, plain language to allow readers

[43]Because challenges associated with a complicated regulatory environment and vendor issues are not directly related to challenges in accessing support from federal agencies, those challenges are not addressed in this section.

[44]Department of Health and Human Services, Food and Drug Administration Center for Devices and Radiological Health, *Best Practices for Communicating Cybersecurity Vulnerabilities to Patients (*Oct. 1, 2021).

[45]Healthcare and Public Health Sector Coordinating Council Cybersecurity Working Group, *MedTech Vulnerability Communications Toolkit* (April 2022).

without a technical background to understand the vulnerability and what steps are required to remediate the vulnerability.

- ASPR officials stated that the agency had worked increasingly with FDA to develop incident-appropriate communication content for vulnerabilities. They added that part of their ongoing efforts will include development and analysis of current communications to the private sector from HHS, CISA, and FBI. These efforts are to evaluate completeness and appropriateness of communications, including intended audience and level of technical sophistication.
- CISA has published resources on its website, including the Healthcare and Public Health Cybersecurity toolkit, which it developed together with HHS and HSCC. The toolkit is intended to consolidate key resources for healthcare and public health organizations at every level, starting with fundamental cyber hygiene steps.

Agency actions to improve awareness of contacts. Agencies are taking actions that could address challenges associated with the lack of awareness of federal contacts. For example:

- FDA has partnered with industry leaders to produce an incident response playbook, which includes federal resources and contacts that are readily available on the internet.[46] FDA officials also stated that they have a shared mailbox and contact information publicly available on the internet, and that they have procedures in place to ensure stakeholders who reach out receive a response.
- CISA has a reporting page intended to allow organizations to, among other things, report incidents. Officials stated that CISA regularly re-evaluates reporting triage processes to ensure that reports are not missed or mis-routed.[47]
- ASPR officials stated that they are working with other agencies and private sector partners to increase coordination and communication and improve awareness of available resources.
- Officials from the Centers for Medicare and Medicaid Services explained that all of its Medicare-participating providers and suppliers are required to have a communication plan. This plan is required to account for interruptions in communications such as cyber-attacks.

[46]MITRE, Medical Device Innovation Consortium, *Playbook for Threat Modeling Medical Devices* (Nov. 30, 2021).

[47]The reporting page can be found at https://www.cisa.gov/report.

Providers are expected to communicate with emergency preparedness contacts and federal partners.

Key Agencies Coordinate on Device Cybersecurity but Do Not Always Follow Leading Practices

A well-developed coordination plan can help ensure that agencies effectively coordinate and avoid fragmentation, duplication, or overlap of work. Prior GAO reports have identified eight leading interagency collaboration practices that, taken together, form a framework for effective coordination and collaboration.[48] Leading practices and key considerations for implementing them include the following:

- **Define common outcomes.** Have the crosscutting challenges or opportunities been identified? Have short- and long-term outcomes been clearly defined? Have the outcomes been reassessed and updated, as needed?
- **Ensure accountability.** What are the ways to monitor, assess, and communicate progress toward the short- and long-term outcomes? Have collaboration-related competencies or performance standards been established against which individual performance can be evaluated? Have the means to recognize and reward accomplishments related to collaboration been established?
- **Bridge organizational cultures**. Have strategies to build trust among participants been developed? Have participating agencies established compatible policies, procedures, and other means to operate across agency boundaries? Have participating agencies agreed on common terminology and definitions?
- **Identify and sustain leadership.** Has a lead agency or individual been identified? If leadership will be shared between one or more agencies, have roles and responsibilities been clearly identified and agreed upon? How will leadership be sustained over the long term?
- **Clarify roles and responsibilities**. Have the roles and responsibilities of the participants been clarified? Has a process for making decisions been agreed upon?
- **Include relevant participants.** Have all relevant participants been included? Do the participants have the appropriate knowledge, skills, and abilities to contribute? Do participants represent diverse perspectives and expertise?
- **Leverage resources and information.** How will the collaboration be resourced through staffing? How will the collaboration be resourced

[48]GAO-23-105520.

through funding? Are methods, tools, or technologies to share relevant data and information being used?

- **Develop and update written guidance and agreements.** If appropriate, have agreements regarding the collaboration been documented? Have ways to continually update or monitor written agreements been developed?

FDA and CISA Have a Documented Collaboration Agreement Addressing Most Leading Practices

FDA and CISA coordinate closely on medical device cybersecurity to fulfill their missions. Of the key agencies with responsibilities over medical device cybersecurity, FDA and CISA are the only pair of agencies that have a documented collaboration agreement.

The documented agreement between FDA and CISA contains several components of the leading practices. For example, the agreement:

- Defines their shared goals. For instance, the agreement states that the goal of the agreement is to share information to enhance mutual awareness, heighten coordination, catalyze standards development, and enhance technical capabilities between the parties.
- Addresses bridging organizational gaps. The leading practices suggest that one way agencies can bridge gaps is by agreeing on common definitions and terminology. The agreement defines the meaning of key terms, including “device” and “medical device manufacturer.”
- Identifies leadership. The agreement lists the responsibilities of each agency and designated CISA to serve as the central medical device vulnerability coordination center and interface with appropriate stakeholders in performance of such duties.
- Defines roles and responsibilities. The agreement lists the responsibilities of each agency. In it, both parties are expected to participate in regular, ad-hoc, and emergency coordination calls to enhance mutual awareness of medical device cybersecurity vulnerabilities and threats to the Healthcare and Public Health sector and device manufacturers operating within it. More specifically, FDA has responsibilities such as providing CISA with draft public releases and commenting on CISA draft advisories and alerts in a timely manner. Similarly, CISA has responsibilities which include, for example, publishing alerts and advisories; coordinating with FDA on the contents of alerts and advisories; and, as an independent third-party, aiding in the evaluation and assessment of the impact of vulnerabilities.

- Addresses leveraging appropriate resources. The agreement states that all activities are subject to the availability of personnel, resources, and funds, and that it does not commit or obligate any funding or resources of either agency.

However, the agreement does not include three leading practices—ensuring accountability, including relevant participants, and developing and updating written guidance and agreements. For example:

- The agreement does not include ways to monitor, assess, and communicate progress on short and long-term outcomes. In addition, the agreement does not establish collaboration-related competencies or performance standards against which individual performance can be evaluated. Further, it does not establish means to recognize and reward accomplishments related to collaboration.
- At the time the agreement was signed in October 2018, CISA was known as the National Protection and Programs Directorate at the Department of Homeland Security and is referred to as such throughout the document. The directorate was replaced by CISA when the Cybersecurity and Infrastructure Security Agency Act of 2018 was signed into law on November 16, 2018.[49]
- FDA and CISA have not updated the agreement since it was originally signed in October 2018. During this time, other changes have occurred. For example, in 2020 FDA developed a standard operating procedure for information sharing with CISA.

Until FDA and CISA collaborate to update their agreement to incorporate missing leading practices, the agency will have less assurance that it will be able to effectively coordinate and avoid fragmentation, duplication, or overlap of work.

Other Key Agencies Coordinated Informally with FDA

Although numerous other key agencies coordinate to support cybersecurity in medical devices, most do so informally and as needed with FDA. These other agencies do not have a direct relationship that FDA and CISA have regarding medical device cybersecurity. Instead,

[49]Pub. L. No. 115-278, 132 Stat. 4168 (codified at 6 U.S.C. § 652).

discussions focus on broader issues; medical devices are a subset of the overall coordination between other agencies.[50]

Agencies generally reported no challenges with an informal or ad-hoc arrangement. For example, numerous other organizations within HHS such as Centers for Medicare and Medicaid Services, Office for the National Coordinator for Health IT, and OCR often defer to FDA as the lead agency in medical device cybersecurity. They mostly receive information from FDA through working groups as they are not a regulator of devices.

Other agencies outside of HHS, including NIST and VA, reported productive collaborative efforts without necessarily needing a documented agreement. Agency officials noted the ad-hoc nature of conversations allowed the agencies flexibility in an otherwise low-coordination scenario. Specifically, NIST cited communication during public meetings as a useful method for coordination. Further, officials stated that FDA has referenced NIST's work, and NIST may recommend publications for FDA to review. In addition, FDA and VA officials described more recent conversations between the two agencies—discussions have included topics such as information sharing on device cybersecurity issues—the intent of these discussions was, among other things, to lay the groundwork for future collaboration. Effective coordination should help ensure cybersecurity in medical devices.

Limitations Exist in Agency Authority Over Medical Device Cybersecurity, but Risks Can Be Mitigated

Although recently enacted legislation provided FDA specific authority over medical device cybersecurity, there are limitations in that authority. However, actions by agencies and healthcare organizations can mitigate risks associated with those limitations.

[50]For example, VA officials stated that the agency had started a working group with other agencies like DHA and Indian Health Service focused on the complications associated with agencies that have to meet security requirements both as healthcare providers and federal entities.

Recent Legislation Enhances FDA's Authority Over Medical Device Cybersecurity

The Consolidated Appropriations Act, 2023, signed into law in December 2022, amends the Federal Food, Drug, and Cosmetic Act. Amendments give FDA additional authority over cybersecurity of medical devices, and, among other things, include requirements for device manufacturers to: [51]

- have plans to monitor, identify, and address, as appropriate, cybersecurity vulnerabilities and exploits;
- design, develop, and maintain processes and procedures to provide a reasonable assurance that the device and related systems are cyber secure; and
- provide the Secretary of Health and Human Services with a software bill of materials.

Limitations Exist in FDA's Authority Over Medical Device Cybersecurity

Although recently enacted legislation enhances cybersecurity in medical devices, limitations in FDA's authority exist. Specifically, the Consolidated Appropriations Act, 2023, did not require medical device manufacturers to address these new cybersecurity requirements in their medical device premarket review submissions until March 2023. As such, a device manufacturer who made a submission before March 2023 would not be subject to the new requirements, unless the manufacturer is submitting a new marketing application for changes to the device.[52]

In addition, there are also limitations in FDA's authority over older legacy devices. For example, once a hospital purchases a device and puts it into the environment, there may be aspects for which FDA has authority, but generally FDA does not regulate healthcare organization usage or maintenance of these devices. For instance, an MRI machine may still be in use decades after it was approved for use by FDA, but its manufacturer

[51]Pub. L. No. 117-328, § 3305, 136 Stat. at 5832 (2022).

[52]In addition, FDA did not expect submissions to include additional requirements until October 2023. This was because FDA released guidance on the new requirements in March 2023 that outlined the expectation for submissions to include the additional requirements by October 1, 2023.

may no longer provide updates that could address evolving cyber threats.[53]

Agency and Healthcare Organization Actions Can Mitigate Risk

FDA officials stated that it is premature to know whether the agency would benefit from additional authorities over the cybersecurity of medical devices. As implementation continues, the agency may identify areas where additional authority may be necessary. Officials from agencies other than FDA stated that their agencies did not need additional authorities over cybersecurity of medical devices. Officials at FDA and other key agencies described actions under current authorities, that mitigate risks associated with any limitations in authority, including devices approved prior to March 2023 and legacy devices. For example:

FDA undertakes premarket and postmarket activities to help ensure medical device cybersecurity. FDA officials stated that regardless of formal requirements, the agency takes into account cybersecurity in assessing medical device submissions for reasonable assurance of safety and effectiveness. FDA has explicitly addressed cybersecurity in medical device guidance. For example, FDA issued cybersecurity guidance applicable to software maintenance actions required to address cybersecurity vulnerabilities for networked medical devices in 2005.[54] Further, once devices have been approved for use, FDA conducts passive surveillance on devices, in which it monitors information sources including internal agency information such as recalls, sector risk management alerts, communications with manufacturers, and CISA alerts.[55]

[53]The Department of Health and Human Services' Office of Civil Rights (OCR), which enforces compliance with the HIPAA Security Rule, does not have authority over certain medical device use cases. OCR officials stated that its role of enforcing the Security Rule with respect to the use of medical devices does not depend on what kind of device is being used, but rather, it depends on whether the entity using the device is a HIPAA-regulated entity. The HIPAA protections and requirements only apply to HIPAA-regulated entities. Therefore, medical devices that are not being used by a HIPAA-regulated entity are not subject to, and protected by, the HIPAA requirements. However, OCR officials stated that the office does not receive reports about medical device cybersecurity issues from non-HIPAA regulated entities.

[54]The guidance stated that the FDA Quality System Regulation in the Code of Federal Regulations, Part 820, applies to software maintenance actions.

[55]Based on the Consolidated Appropriations Act, 2023, FDA looks at design, software bill of materials, threat modeling, security control testing, among other cybersecurity areas.

In December 2016, FDA issued guidance on postmarket management of cybersecurity in medical devices, including legacy devices.[56] The guidance states that manufacturers of devices should remediate uncontrolled risks as quickly as possible.[57] In addition, the guidance states that as soon as possible, but not later than 30 days after learning of a vulnerability, the manufacturer is to communicate with healthcare organizations and its user community regarding the vulnerability. The manufacturer is to identify interim compensating controls and develop a remediation plan. Further, as soon as possible but no later than 60 days after learning of the vulnerability, the manufacturer is to fix the vulnerability, validate the change, and distribute the fix to healthcare organizations and its user community such that the risk is brought down to an acceptable level.

As an example, in September 2022, both CISA and FDA posted alerts associated with an insulin pump. The alerts cited cybersecurity risk associated with the communication protocol for the pump system that could allow unauthorized access to the pump system. If unauthorized access were to occur, the pump's communication protocol could be compromised, which may cause the pump to deliver too much or too little insulin. The device manufacturer informed users of this cybersecurity risk and included actions and recommendations for users to take.

Further, FDA's guidance states that in the absence of remediation, a device with uncontrolled risk of patient harm may be considered to have a reasonable probability that use of, or exposure to, the product will cause serious adverse health consequences or death. As such, the guidance states that the device may be considered in violation of the Federal Food, Drug, and Cosmetic Act and subject to enforcement or other action. FDA officials stated that the agency is aware of such incidents, and works with manufacturers to address issues, including through voluntary recalls. In some circumstances, FDA has also issued warning letters to manufacturers.

FDA continues working with federal partners on medical device cybersecurity. FDA officials stated that the agency has grown and

[56]Food and Drug Administration, *Postmarket Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff* (Silver Spring, MD: Dec. 28, 2016).

[57]An uncontrolled risk is present when there is unacceptable residual risk of patient harm due to insufficient risk mitigations and compensating controls.

strengthened medical device policy mechanisms with internal resources and with its federal partners such as CISA, HHS, and FBI, as well as HSCC. FDA officials stated that the agency also looks at lessons learned from other critical infrastructure sectors and participates in a cybersecurity regulators forum for sharing of information and best practices.

Further, in August 2020, FDA developed a standard operating procedure to detail FDA's roles and responsibilities in sharing information with CISA.[58] It covers, among other things, the coordination and participation in regular, ad-hoc, and emergency coordination calls with CISA to enhance mutual awareness of medical device cybersecurity vulnerabilities and to facilitate resolutions to vulnerability coordination issues.[59] FDA officials stated that the agencies have held three emergency coordination meetings since 2019.

Healthcare organizations can take actions to mitigate risks. In addition to federal agency efforts, healthcare organizations can take actions to mitigate cybersecurity risks regarding the use and maintenance of devices. For example, if a legacy device can no longer be protected against current cyber threats, a healthcare organization could separate the device from other devices on the hospital's network to reduce risk. In addition, a healthcare organization could pay for additional vendor support if that support is available or replace the device entirely.

Conclusions

As the lead agency responsible for the cybersecurity of medical devices, FDA facilitates collaboration with other federal agencies. FDA developed a documented coordination agreement with CISA to support cybersecurity of medical devices; however, the agreement is outdated and does not reflect organizational and procedural changes that have occurred over the last 5 years. By updating its written agreement with CISA, FDA can enhance coordination and help ensure clarity of current roles in addressing medical device cybersecurity. Further, although limitations in

[58]The development of a standard operating procedure of this nature was a requirement in FDA's original memorandum of agreement with the Department of Homeland Security as outlined above.

[59]The standard operating procedure requires that when necessary, FDA request emergency coordination calls with CISA personnel to address issues that arise outside of agencies' regularly scheduled calls. The standard operating procedure also requires that FDA ensure adequate and appropriate FDA staff are available when a request for an emergency coordination call originates from CISA.

authority exist for older devices, FDA has taken actions to mitigate the risks associated with these limitations.

Recommendations for Executive Action

We are making one recommendation each to the Food and Drug Administration and the Cybersecurity and Infrastructure Security Agency:

The Commissioner of Food and Drugs should work with the Cybersecurity and Infrastructure Security Agency to update the agencies' agreement to reflect organizational and procedural changes that have occurred. (Recommendation 1)

The Director of the Cybersecurity and Infrastructure Security Agency should work with the Food and Drug Administration to update the agencies' agreement to reflect organizational and procedural changes that have occurred. (Recommendation 2)

Agency Comments and Our Evaluation

We requested comments on a draft of this report from the 11 agencies we selected for our review. In response, the two agencies to which we made recommendations provided comments agreeing with the recommendations. In addition, one agency to which we did not make a recommendation provided comments on the draft report. The remaining agencies did not provide any comments on the draft report.

The Department of Health and Human Services (HHS) responded on behalf of the Food and Drug Administration (FDA) in written comments which are reprinted in appendix III. In its comments, the department concurred with our recommendation and stated that it will begin working with the Cybersecurity and Infrastructure Security Agency (CISA) to update the agencies' agreement to reflect organization and procedural updates that have occurred.

The Department of Homeland Security responded on behalf of CISA and provided written comments which are reprinted in appendix IV. In its comments, the department concurred with our recommendation. The department stated that the agency is proud to work closely with HHS and FDA to deliver tools, resources, training, and information that can help organizations in the Healthcare and Public Health sector. The department also stated that CISA coordinates closely with FDA to conduct coordinated vulnerability disclosure of medical device vulnerability information, and also remains committed to increasing the cybersecurity of medical devices being used in the sector. In addition, the department stated that CISA will work with FDA to update the agencies' information

sharing agreements, and procedures as appropriate, with an estimated completion date in June 2024.

While we did not make recommendations to the Veterans Health Administration (VHA), a component of the Department of Veterans Affairs (VA), provided written comments, which are reprinted in appendix V. In its comments, the department stated that CISA, the National Institute of Standards and Technology (NIST), and the Office of Management and Budget (OMB) do not have a documented collaboration agreement with any federal healthcare delivery organizations, such as the Indian Health Service, National Institutes of Health, or VHA. The department further stated that IT policy that CISA, NIST, and OMB pass down to federal healthcare delivery organizations inadvertently includes medical devices that do not readily conform to tradition IT policy. According to the department, this has made installation, configurations, and operation of networked medical devices more difficult and often has a direct impact on patient care.

We agree that this topic is very important, but it was not included in the scope of our review. However, we point out that documented agreements are only considered part of leading collaboration practices when they are deemed appropriate. In this report, we also note that VA officials stated that the department had started a working group with other agencies, such as Indian Health Service, focused on the complications associated with agencies that have to meet security requirements both as healthcare providers and federal entities. These agencies can coordinate with CISA, NIST, and OMB as they work together moving forward and determine whether a documented agreement is appropriate or not.

In addition to the aforementioned responses, officials from the remaining agencies or their relevant departments reported that they did not have any comments on the draft report. Specifically, we received emails from liaisons at the Department of Defense, for which the Defense Health Agency is a component; the Department of Justice, for which FBI is a component; and the National Institute of Standards and Technology. In addition, the Department of Health and Human Services, for which the Administration for Strategic Preparedness and Response, Center for Medicare and Medicaid Services, and Office of the National Coordinator for Health IT are components, stated that those components did not have any comments on the draft report.

In addition, several agencies provided technical comments, which we addressed as appropriate.

We are sending copies of this report to the appropriate congressional committees, the Commissioner of Food and Drugs, the Director of the Cybersecurity and Infrastructure Security Agency, and other interested parties. In addition, the report is available at no charge on the GAO website at https://www.gao.gov.

If you or your staff have 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 VI.

Jennifer R. Franks
Director, Center for Enhanced Cybersecurity
Information Technology and Cybersecurity

Appendix I: Objectives, Scope, and Methodology

The objectives for this review were to determine the extent to which (1) relevant non-federal entities are facing challenges in accessing federal support on medical device cybersecurity, (2) federal agencies have addressed identified challenges, (3) key agencies are coordinating on medical device cybersecurity, and (4) limitations exist in agencies' authority over medical device cybersecurity.

For the first objective, we selected a sample of non-federal entities by reviewing a list of members in the Healthcare and Public Health Sector Coordinating Council (HSCC) Cybersecurity Working Group and focusing on large associations of medical device manufacturers, health systems, and healthcare providers.[1]

We then reviewed the mission statements of the large associations to determine which of those associations appeared to support membership that manufactured, prescribed, or otherwise utilized medical devices that may experience cybersecurity threats. For the 11 associations that met this criterion, we performed semi-structured interviews with six of the entities.[2]

During our interviews with association representatives, we asked for additional membership who might be interested in speaking with us to further expand the information we could collect. We asked for a cross section of organizations based on size, to obtain a variety of different perspectives. We held interviews with an additional eight entities.[3]

To obtain perspectives from patients, we asked the federal agencies in the scope of our review (described below) if they were aware of any patient advocacy organizations who may have perspectives pertinent to our review. We also relied on GAO subject matter expert guidance to

[1]The mission of the HSCC Cyber Working Group is to collaborate with the Department of Health and Human Services and other federal agencies to identify and mitigate systemic risks that affect patient safety, security, and privacy, and consequently, national confidence in the health care system. Primary HSCC outputs for risk mitigation are the development of recommendations, best practices and guidance for enterprise cybersecurity improvements, as well as advice to government partners about policy and regulatory solutions that facilitate mitigation of cybersecurity threats to the sector.

[2]The remaining entities either told us that they did not have relevant answers to our questions or did not respond to our outreach.

[3]In addition to the interviews with eight suggested entities, we also held an interview with the Executive Director of the HSCC Cyber Working Group.

develop a list of patient organizations to interview. We held semi-structured interviews with three of those entities.[4]

We interviewed a total of 25 non-federal entities.[5] The complete list of non-federal entities is available in Appendix II. After holding all of the interviews, we performed an analysis of the interview results to identify challenges in accessing federal support for medical device cybersecurity.[6]

Regarding the second and third objectives, we first selected a set of key federal agencies with responsibility for medical device cybersecurity. We did so based on a review of previous GAO work, public reports by federal agencies, and initial conversations with the Food and Drug Administration (FDA) and Cybersecurity and Infrastructure Security Agency (CISA), who we had initially determined to be in scope for the review.

After consideration of our background research and discussion with GAO subject matter experts, we selected the following 11 agencies for our review:

- National Institute of Standards and Technology at the Department of Commerce,
- Administration for Strategic Preparedness and Response at the Department of Health and Human Services,
- Centers for Medicare and Medicaid Services at the Department of Health and Human Services,
- Food and Drug Administration at the Department of Health and Human Services,
- Indian Health Service at the Department of Health and Human Services,

[4]Although we reached out to more than three patient organizations, we were only able to schedule interviews with three of the organizations due to the time it took to schedule the interviews during our audit work.

[5]During our interviews with the entities, in some cases additional participants attended who represented the views of additional entities. As such, we also interviewed representatives from seven additional entities for a total of 25 entities in total.

[6]Specifically, one analyst first developed a list of challenges based on the results of the interviews. A second analyst then reviewed the first analyst's work to ensure that both analysts concurred with a final list of challenges.

- Office for Civil Rights at the Department of Health and Human Services,
- Office of the National Coordinator for Health Information Technology at the Department of Health and Human Services,
- Cybersecurity and Infrastructure Security Agency at the Department of Homeland Security,
- Federal Bureau of Investigation at the Department of Justice,
- Veterans Health Administration at the Department of Veterans Affairs, and
- Defense Health Agency at the Department of Defense

For the second objective, we reviewed agency guidance and information available on agency websites. We also held interviews with agency officials responsible for medical device cybersecurity. The interviews were intended to help understand to what extent agencies had heard about, and taken action related to, challenges identified in the engagement's first objective.

For the third objective, we requested and reviewed any guidance that the selected agencies had developed concerning medical device cybersecurity. We also reviewed any memorandums of understanding developed by agencies that governed agency coordination regarding medical device cybersecurity.[7] Further, we requested and reviewed meeting minutes between collaborating agencies. We assessed agency responses and documentation against leading practices in interagency collaboration[8] and fragmentation, overlap, and duplication.[9] We also held interviews with the selected agencies to understand each agency's role in supporting medical device cybersecurity, as well as to understand what interactions the agencies had with other federal entities.

To answer the fourth objective, we reviewed relevant legislation, regulations, and guidance to understand the scope of agencies' authority

[7]A memorandum of agreement, or memorandum of understanding, is a document describing a partnership between two or more parties that have agreed to cooperate to meet an agreed objective or complete a project.

[8]GAO, *Government Performance Management: Leading Practices to Enhance Interagency Collaboration and Address Crosscutting Challenges*, GAO-23-105520 (Washington, D.C.: May 24, 2023).

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

over the cybersecurity of medical devices. Specifically, we reviewed the following:

- Federal Food, Drug, and Cosmetic Act,
- Consolidated Appropriations Act, 2023,[10]
- Health Insurance Portability and Accountability Act (HIPAA) and the HIPAA Security Rule,[11] and
- Federal agency guidance about medical device cybersecurity, including FDA's draft premarket cybersecurity guidance[12]

We also held interviews with key agency officials to further understand the scope and application of their authority regarding the cybersecurity of medical devices, and inquired about agency determinations that there are limitations or potential limitations in authority. Where agencies identified actions to mitigate risk associated with potential limitations, we reviewed documentation associated with FDA's postmarket guidance and coordination with other agencies.[13]

We conducted this performance audit from March 2023 to December 2023 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.

[10]Pub. L No. 117-328, which amends the Federal Food, Drug, and Cosmetic Act, 21 U.S.C. 351 et. seq.

[11]Pub. L. No. 104-191, and the HIPAA Security Rule, 45 C.F.R. Part 164 Subpart C.

[12]87 Fed. Reg. 20873

[13]Postmarket refers to the time period after introduction of a device into the market for patient and provider use.

Appendix II: Non-Federal Entity Interviewees

As described in Appendix I, we interviewed a total of 25 non-federal entities to obtain their views on challenges in accessing federal support when addressing cybersecurity vulnerabilities that may threaten medical devices. Non-federal entities included the following:

- American Hospital Association,
- American Medical Association,
- Association for Executives in Healthcare Information Security (College of Healthcare Information Management Executives),
- AtlantiCare Health System,
- Baptist Health Jacksonville,
- Becton Dickinson,
- Biohacking Village,
- Cuero Regional Health,
- Deborah Heart and Lung Center,
- Health Sector Coordinating Council Cyber Working Group,
- Johnson & Johnson,
- Lawrence Memorial Hospital,
- Medical Device Manufacturers Association,
- Medical Imaging and Technology Alliance,
- Memorial Community Hospital,
- Nemaha County Hospital,
- New Jersey Hospital Association,
- Northwell Health,
- Patient Engagement Advisory Committee,
- Philips Healthcare,
- Public Citizen,
- Rady Children's Hospital San Diego,
- Siemens Healthineers,
- Speare Memorial Hospital, and
- St. Joseph Health.

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

December 1, 2023

Jennifer R. Franks
Director, Center for Enhanced Cybersecurity
Information Technology and 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, **"Medical Device Cybersecurity: Agencies Need to Update Agreement to Ensure Effective Coordination" (GAO-24-106683).**

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

Sincerely,

Melanie Anne Egorin

Melanie Anne Egorin, PhD
Assistant Secretary for Legislation

Attachment

GENERAL COMMENTS OF THE DEPARTMENT OF HEALTH & HUMAN SERVICES ON THE GOVERNMENT ACCOUNTABILITY OFFICE'S DRAFT REPORT ENTITLED – MEDICAL DEVICE CYBERSECURITY: AGENCIES NEED TO UPDATE AGREEMENT TO ENSURE EFFECTIVE COORDINATION (GAO-24-106683)

The Department appreciates the opportunity to review and comment on this draft report.

GAO Recommendation 1
The Commissioner of Food and Drugs should work with the Cybersecurity and Infrastructure Security Agency to update the agencies' agreement to reflect organization and procedural updates that have occurred.

HHS Response
HHS concurs with this recommendation and will begin working with CISA to update the information sharing agreement that is in place.

Appendix IV: Comments from the Department of Homeland Security

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

December 8, 2023

Jennifer R. Franks
Director, Center for Enhanced Cybersecurity
Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548-0001

Re: Management Response to Draft Report GAO-24-106683, "MEDICAL DEVICE CYBERSECURITY: Agencies Need to Update Agreement to Ensure Effective Coordination"

Dear Ms. Franks,

Thank you for the opportunity to comment on this draft report. The U.S. Department of Homeland Security (DHS or the Department) appreciates the U.S. Government Accountability Office's (GAO) work in planning and conducting its review and issuing this report.

DHS leadership is pleased to note GAO's recognition of the collaboration between the Cybersecurity and Infrastructure Security Agency (CISA) and the Department of Health and Human Services (HHS), including the Food and Drug Administration (FDA), to protect the critical Healthcare and Public Health (HPH) sector and respond to medical device vulnerabilities. Specifically, GAO noted that CISA and FDA developed an agreement addressing most leading practices for collaboration to manage medical device cybersecurity.

Although medical devices have not typically been exploited to disrupt clinical operations in hospitals, they are still a source of significant concern due to the threats they can introduce to hospital cybersecurity. As the Sector Risk Management Agency, HHS has a lead role in improving the safety, resilience, and security of the HPH sector. CISA is proud to work closely with HHS and FDA to deliver tools, resources, training, and information that can help organizations within this sector. For example, in October 2023, CISA partnered with HHS and the Health Sector Coordinating Council to release the HPH Cybersecurity Toolkit, which consolidates key resources such as services, guidance,

and training, to help this important component of the nation's critical infrastructure reduce cyber risk and the likelihood of successful cyber incursions.

CISA also coordinates closely with FDA to conduct coordinated vulnerability disclosure of medical device vulnerability information, which allows: (1) CISA to better understand medical device vulnerabilities throughout the disclosure process; and (2) FDA to conduct patient impact analysis. This pre-disclosure coordination also allows both parties, along with the security researchers who report vulnerabilities and the manufacturer responsible for providing mitigations, to coordinate public messaging prior to public disclosure of medical device vulnerabilities and their associated mitigations. DHS remains committed to increasing the cybersecurity of medical devices being used in the HPH sector.

The draft report contained two recommendations, including one for DHS with which the Department concurs. Enclosed find our detailed response to the recommendation. DHS previously submitted technical comments under a separate cover for GAO's consideration.

Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions. We look forward to working with you again in the future

Sincerely,

JIM H CRUMPACKER

Digitally signed by JIM H CRUMPACKER
Date: 2023.12.08 06:25:27 -05'00'

JIM H. CRUMPACKER, CIA, CFE
Director
Departmental GAO-OIG Liaison Office

Enclosure

2

Enclosure: Management Response to Recommendation Contained in GAO-24-106683

GAO recommended that the Director of CISA:

Recommendation 2: Work with the Food and Drug Administration to update the agencies' agreement to reflect organizational and procedural updates that have occurred.

Response: Concur. CISA's Cybersecurity Division will work with FDA to update the agencies' information sharing agreements, and procedures as appropriate, to accurately capture current organizations, authorities, and roles in in addressing medical device and HPH sector cybersecurity. Estimated Completion Date: June 28, 2024.

3

Appendix V: Comments from the Department of Veterans Affairs

DEPARTMENT OF VETERANS AFFAIRS
WASHINGTON

December 13, 2023

Ms. Jennifer R. Franks
Director, Center for Enhanced Cybersecurity
Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Ms. Franks:

The Department of Veterans Affairs (VA) has reviewed the Government Accountability Office (GAO) draft report: ***Medical Device Cybersecurity: Agencies Need to Update Agreement to Ensure Effective Coordination*** (GAO-24-106683).

The Cybersecurity and Infrastructure Security Agency (CISA), National Institute of Standards and Technology (NIST), and Office of Management and Budget (OMB) do not have a documented collaboration agreement with any other Federal health care delivery organization (HDO), such as Indian Health Service, National Institute of Health, or Veterans Health Administration.

Before implementing blanket information technology (IT) policies, CISA, NIST, and OMB should communicate with Federal HDOs to assess impacts to medical device networks and direct patient care. The IT policy that CISA, NIST, and OMB pass down to Federal HDOs often inadvertently includes medical devices that do not readily conform to traditional IT policy. This creates substantial challenges as VA's Office of Information and Technology seeks to apply federally mandated standards to medical systems that are not designed to meet those standards. This has made installation, configurations, and operation of networked medical devices very difficult and often has a direct impact on patient care.

VA appreciates the opportunity to comment on your draft report.

Sincerely,

Kimberly Jackson
Chief of Staff

Appendix VI: GAO Contacts and Staff Acknowledgments

GAO Contact

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

Staff Acknowledgments

In addition to the individual named above, Jeffrey Knott (Assistant Director), Kevin Smith (Analyst-in-Charge), Brandon Berney, Kisa Bushyeager, Chris Businsky, Donna Epler, Catherine Fan, Smith Julmisse, Monica Perez-Nelson, and Walter Vance 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

A. Nicole Clowers, Managing Director, ClowersA@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, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548