



December 2022

CRITICAL INFRASTRUCTURE

Actions Needed to Better Secure Internet-Connected Devices

GAO Highlights

Highlights of [GAO-23-105327](#), a report to congressional committees

Why GAO Did This Study

Cyber threats to critical infrastructure IoT and OT represent a significant national security challenge. Recent incidents—such as the ransomware attacks targeting health care and essential services during the COVID-19 pandemic—illustrate the cyber threats facing the nation’s critical infrastructure. Congress included provisions in the IoT Cybersecurity Improvement Act of 2020 for GAO to report on IoT and OT cybersecurity efforts.

This report (1) describes overall federal IoT and OT cybersecurity initiatives; (2) assesses actions of selected federal agencies with a lead sector responsibility for enhancing IoT and OT cybersecurity; and (3) identifies leading guidance for addressing IoT cybersecurity and determines the status of OMB’s process for waiving cybersecurity requirements for IoT devices. To describe overall initiatives, GAO analyzed pertinent guidance and related documentation from several federal agencies.

To assess lead agency actions, GAO first identified the six critical infrastructure sectors considered to have the greatest risk of cyber compromise. From these six, GAO then selected for review three sectors that had extensive use of IoT and OT devices and systems. The three sectors were energy, healthcare and public health, and transportation systems. For each of these, GAO analyzed documentation, interviewed sector officials, and compared lead agency actions to federal requirements.

View [GAO-23-105327](#). For more information, contact David B. Hinchman at (214) 777-5719 or hinchmand@gao.gov.

December 2022

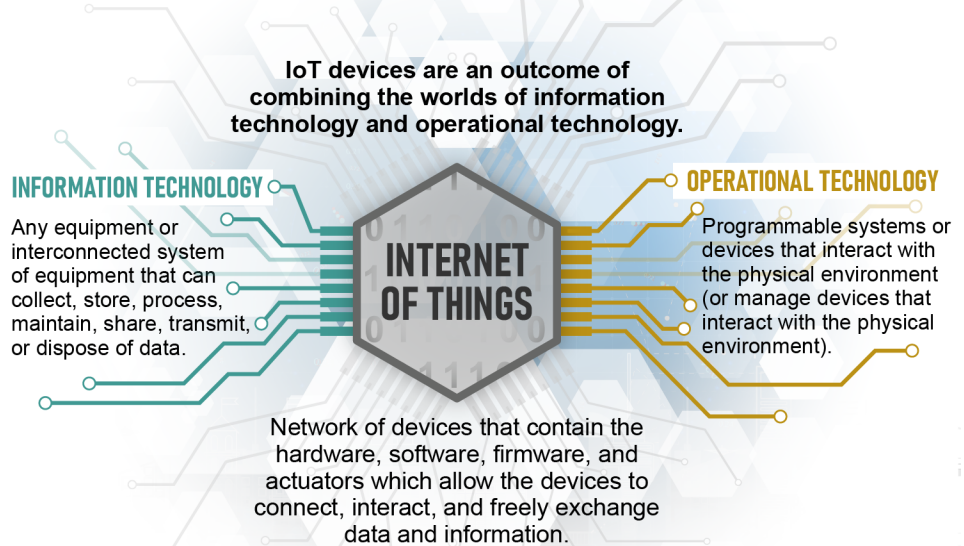
CRITICAL INFRASTRUCTURE

Actions Needed to Better Secure Internet-Connected Devices

What GAO Found

The nation’s critical infrastructure sectors rely on electronic systems, including Internet of Things (IoT) and operational technology (OT) devices and systems. IoT generally refers to the technologies and devices that allow for the network connection and interaction of a wide array of “things,” throughout such places as buildings, transportation infrastructure, or homes. OT are programmable systems or devices that interact with the physical environment, such as building automation systems that control machines to regulate and monitor temperature.

Figure: Overview of Connected IT, Internet of Things (IoT), and Operational Technology



Source: GAO; images: ZinetroN/stock.adobe.com, Stockgiu/stock.adobe.com, yershovoleksandr/stock.adobe.com. | GAO-23-105327

To help federal agencies and private entities manage the cybersecurity risks associated with IoT and OT, the Department of Homeland Security’s Cybersecurity and Infrastructure Security Agency (CISA) and the National Institute of Standards and Technology (NIST) have issued guidance and provided resources. Specifically, CISA has published guidance, initiated programs, issued alerts and advisories on vulnerabilities affecting IoT and OT devices, and established working groups on OT. NIST has published several guidance documents on IoT and OT, maintained a center of cybersecurity excellence, and established numerous working groups. In addition, the Federal Acquisition Regulatory Council is considering updates to the Federal Acquisition Regulation to better manage IoT and OT cybersecurity risks.

Selected federal agencies with a lead role have reported various cybersecurity initiatives to help protect three critical infrastructure sectors with extensive use of IoT or OT devices and systems.

GAO also analyzed documentation, interviewed officials from the selected sectors, and compared those sector's cybersecurity efforts to federal requirements. GAO also interviewed OMB officials on the status of the mandated waiver process.

What GAO Recommends

GAO is making eight recommendations to the lead agencies of the reviewed sectors—the Departments of Energy, Health and Human Services, Homeland Security, and Transportation. GAO is recommending that each department (1) establish and use metrics to assess the effectiveness of sector IoT and OT cybersecurity efforts and (2) evaluate sector IoT and OT cybersecurity risks. GAO is also making one recommendation to OMB to expeditiously establish the required IoT cybersecurity waiver process.

The Departments of Homeland Security and Transportation concurred with the recommendations while Energy said it would not respond to the recommendations until after further coordination with other agencies. Health and Human Services neither agreed nor disagreed with the recommendations but noted planned actions. Specifically, the department said it planned to update its sector-specific plan but asserted that it cannot compel adoption of the plan in the private sector. GAO recognizes the voluntary character of the relationship between the department and the critical infrastructure sector. However, establishing IoT and OT specific metrics will provide a basis for the department to establish accountability, document actual performance, promote effective management, and provide a feedback mechanism to inform decision-making.

OMB stated that the agency is targeting November 2022 for release of guidance on the waiver process. As of November 22, 2022, OMB had not yet issued this guidance.

Title: Sector Lead Agencies' Internet of Things (IoT) or Operational Technology (OT) Cybersecurity Initiatives

Sector (Lead Federal Agency)	Examples of IoT or OT Initiatives
Energy (Department of Energy)	<p>Considerations for OT Cybersecurity Monitoring Technologies guidance provides suggested evaluation considerations for technologies to monitor OT cybersecurity of systems that, for example, distribute electricity through the grid.</p> <p>Cybersecurity for the Operational Technology Environment methodology aims to enhance energy sector threat detection of anomalous behavior in OT networks, such as electricity distribution networks.</p>
Healthcare and public health (Department of Health and Human Services)	<p>Pre-market Guidance for Management of Cybersecurity identifies issues related to cybersecurity for manufacturers to consider in the design and development of their medical devices, such as diagnostic equipment.</p> <p>Post-market Management of Cybersecurity in Medical Devices provides recommendations for managing cybersecurity vulnerabilities for marketed and distributed medical devices, such as infusion pumps.</p>
Transportation systems (Departments of Homeland Security and Transportation)	<p>Surface Transportation Cybersecurity Toolkit is designed to provide informative cyber risk management tools and resources for control systems that, for example, function on the mechanics of the vessel.</p> <p>Department of Homeland Security's Transportation Security Administration's Enhancing Rail Cybersecurity Directive requires actions, such as conducting a cybersecurity vulnerability assessment and developing of cybersecurity incident response plans for higher risk railroads.</p>

Source: GAO analysis of agency documentation | GAO-23-105327

However, none of the selected lead agencies had developed metrics to assess the effectiveness of their efforts. Further, the agencies had not conducted IoT and OT cybersecurity risk assessments. Both of these activities are best practices. Lead agency officials noted difficulty assessing program effectiveness when relying on voluntary information from sector entities. Nevertheless, without attempts to measure effectiveness and assess risks of IoT and OT, the success of initiatives intended to mitigate risks is unknown.

The Internet of Things Cybersecurity Improvement Act of 2020 generally prohibits agencies from procuring or using an IoT device after December 4, 2022, if that device is considered non-compliant with NIST-developed standards. Pursuant to the act, in June 2021 NIST issued a draft guidance document that, among other things, provides information for agencies, companies and industry to receive reported vulnerabilities and for organizations to report found vulnerabilities. The act also requires the Office of Management and Budget (OMB) to establish a standardized process for federal agencies to waive the prohibition on procuring or using non-compliant IoT devices if waiver criteria detailed in the act are met.

As of November 22, 2022, OMB had not yet developed the mandated process for waiving the prohibition on procuring or using non-compliant IoT devices. OMB officials noted that the waiver process requires coordination and data gathering with other entities. According to OMB, it is targeting November 2022 for the release of guidance on the waiver process. Given the act's restrictions on agency use of non-compliant IoT devices beginning in December 2022, the lack of a uniform waiver process could result in a range of inconsistent actions across agencies.

Contents

Letter		1
	Background	4
	Federal Agencies Have Issued Guidance for Managing IoT and OT Cybersecurity Risks	22
	Selected SRMAs Did Not Measure Effectiveness of IoT and OT Efforts or Assess Cybersecurity Risks	35
	NIST Has Issued Guidance, but OMB Has Not Established a Required Cybersecurity Waiver Process	48
	Conclusions	51
	Recommendations for Executive Action	52
	Agency Comments and Our Evaluation	53
Appendix I	Objectives, Scope, and Methodology	58
Appendix II	National Institute of Standards and Technology Publications and Guidance on Internet of Things and Operational Technology	62
Appendix III	Comments from the Department of Health and Human Services	67
Appendix IV	Comments from the Department of Homeland Security	69
Appendix V	GAO Contact and Staff Acknowledgments	72
Tables		
	Table 1: Examples of Common and Damaging Types of Cyberattacks	10
	Table 2: Selected Critical Infrastructure Sectors' Internet of Things (IoT) Environment	18
	Table 3: Selected Critical Infrastructure Sectors' Operational Technology (OT) Environment	19
	Table 4: Selected Cybersecurity and Infrastructure Security Agency (CISA) Internet of Things (IoT) Cybersecurity Publications	24

Table 5: Selected Cybersecurity and Infrastructure Security Agency (CISA) Operational Technology (OT) Cybersecurity Publications	25
Table 6: Validated Architecture Design Reviews by Sector and Fiscal Year (FY)	27
Table 7: National Institute of Standards and Technology (NIST) Key Publications on Internet of Things (IoT) Cybersecurity	30
Table 8: National Institute of Standards and Technology (NIST) Publications on Operational Technology (OT) Cybersecurity	31
Table 9: Examples of Potential Changes to the Federal Acquisition Regulation (FAR) Affecting IoT and OT Cybersecurity (September 2022)	34
Table 10: National Institute of Standards and Technology (NIST) Publications and Guidance on the Internet of Things and Operational Technology	62
Table 11: National Institute of Standards and Technology (NIST) National Cybersecurity Center of Excellence (NCCoE) Publications on the Cybersecurity of Internet of Things (IoT) and Operational Technology (OT) Devices	65

Figures

Figure 1: Intersection of IT, Internet of Things (IoT), and Operational Technology	9
Figure 2: Theoretical Depiction of a Botnet Attack on the Electrical Grid	12
Figure 3: Critical Infrastructure Sectors and Related Sector Risk Management Agencies	17

Abbreviations

CESER	Cybersecurity, Energy Security, and Emergency Response
CIO	Chief Information Officer
CISA	Cybersecurity and Infrastructure Security Agency
DARC	Defense Acquisition Regulations Council
DHS	Department of Homeland Security
DOD	Department of Defense
DOE	Department of Energy
DOT	Department of Transportation
EPA	Environmental Protection Agency
FAR	Federal Acquisition Regulation
FDA	Food and Drug Administration
GSA	General Services Administration
HHS	Department of Health and Human Services
ICS	industrial control systems
ICS-CERT	industrial control systems Cyber Emergency Response Team
IIoT	Industrial Internet of Things
IoT	Internet of Things
IR	interagency report
ISAC	Information Sharing and Analysis Center
MUD	manufacturer usage description
NASA	National Aeronautics and Space Administration
NCCoE	National Cybersecurity Center of Excellence
NDAA	National Defense Authorization Act
NIST	National Institute of Standards and Technology
NIST IR	NIST interagency report
NSTAC	National Security Telecommunications Advisory Committee
OMB	Office of Management and Budget
OT	operational technology
SCADA	Supervisory Control and Data Acquisition
SCC	sector coordinating council
SP	special publication
SQL	structured query language
SRMA	sector risk management agency
TSA	Transportation Security Administration
USDA	United States Department of Agriculture
US-CERT	United States Computer Emergency Readiness Team

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.



December 1, 2022

Congressional Committees

The nation’s 16 critical infrastructure sectors provide essential services, such as electricity, health care, and transportation.¹ These sectors rely on electronic systems, including Internet of Things (IoT)² and operational technology (OT)³ devices and systems, and data to support their missions. However, cyber threats to critical infrastructure—like the May 2021 ransomware cyberattack on an American oil pipeline system that led to regional gas shortages—continue to increase and represent a significant national security challenge.

In 2020, we surveyed 90 federal agencies, and 56 reported using IoT technologies. These agencies used IoT to control or monitor equipment or systems, control access to facilities, or track physical assets.⁴ Much of today’s OT evolved from the insertion of IT capabilities into existing physical systems, often replacing or supplementing physical control mechanisms. While this move toward IoT and OT increases the

¹The term “critical infrastructure” refers to 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 matters. 42 U.S.C. § 5195c(e). Federal policy identifies 16 critical infrastructure sectors: chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; healthcare and public health; information technology; nuclear reactors, materials and waste; transportation systems; and water and wastewater systems.

²IoT generally refers to the technologies and devices that allow for the network connection and interaction of a wide array of devices, or “things,” throughout such places as buildings, vehicles, transportation infrastructure, or homes.

³The National Institute of Standards and Technology defines OT as programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment).

⁴GAO, *Internet of Things: Information on Use by Federal Agencies*, [GAO-20-577](#) (Washington, D.C.: August 13, 2020).

connectivity of these systems, it also creates a greater need for these systems' adaptability, resilience, safety, and security.⁵

The Internet of Things Cybersecurity Improvement Act of 2020⁶ includes a provision for us to report on IoT and OT cybersecurity efforts. It also includes a provision for us to conduct a series of reviews on best practices for IoT procurement and on a federal IoT cybersecurity requirement waiver process.⁷ Our specific objectives for this review were to (1) describe overall federal initiatives for managing cybersecurity risks associated with IoT and OT devices; (2) assess actions of selected sector risk management agencies (SRMA) to enhance the cybersecurity of their sectors' IoT and OT environments;⁸ and (3) identify leading guidance for addressing IoT cybersecurity, and determine the status of Office of Management and Budget's (OMB) process for waiving cybersecurity requirements for such devices.

To address our first objective, we obtained and described overall IoT and OT cybersecurity guidance issued or initiatives led, by federal agencies with cybersecurity or acquisition responsibilities. These included OMB, the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA), the General Services Administration (GSA), the National Institute of Standards and Technology (NIST), and the National Aeronautics and Space Administration (NASA).⁹

⁵National Institute of Standards and Technology, *Guide to Industrial Control Systems (ICS) Security*, Special Publication 800-82 Revision 2, (May 2015) and *Guide to Operational Technology Security*, NIST Special Publication 800-82 Revision 3 (Draft), (April 2022).

⁶Internet of Things Cybersecurity Improvement Act of 2020, Pub. L. No. 116-207. 134 Stat. 1001 (Dec. 4, 2020). The statute is also named the IoT Cybersecurity Improvement Act of 2020.

⁷The Internet of Things Cybersecurity Improvement Act of 2020 included a provision for GAO to report biennially on IoT procurement best practices and a cybersecurity IoT waiver process. Subsequent reviews are due to Congress in December 2024 and December 2026.

⁸SRMAs lead, facilitate, and support, the security and resilience programs and associated activities of their designated critical infrastructure sector.

⁹The General Services Administration and National Aeronautics and Space Administration are two of the four members of the Federal Acquisition Regulatory Council. The other two members are the Department of Defense and the Office of Federal Procurement Policy in the Office of Management and Budget.

To address the second objective, we first identified the six critical infrastructure sectors, identified in the 2018 National Cyber Strategy of the United States of America, as having the greatest risk of cyber compromise.¹⁰ The six sectors were: communications, energy, information technology, healthcare and public health, financial services, and transportation systems. We then met with SRMA officials and with industry representatives, including sector coordinating councils (SCC)¹¹ and Information Sharing and Analysis Centers (ISAC)¹² for the respective sectors to determine the extent to which IoT and OT devices and systems are used within their sector. Using this information, we then selected the energy, healthcare and public health, and transportation systems sectors for further review. These sectors use IoT, OT, or both types of devices extensively.¹³

We evaluated documentation on IoT and OT cybersecurity efforts led by the selected SRMAs or coordinating councils. We also interviewed officials to determine the extent to which they have cybersecurity-related processes in place to manage cybersecurity risks to IoT and OT environments for their sectors. We compared these efforts to requirements and best practices in the National Defense Authorization Act (NDAA) for Fiscal Year 2021,¹⁴ Presidential Policy Directive 21,¹⁵ and

¹⁰The White House, *National Cyber Strategy of the United States of America* (Washington, D.C.: September 2018).

¹¹Sector coordinating councils (SCC) are formed as self-organized, self-governing councils that enable critical infrastructure owners and operators, their trade associations, and other industry representatives to interact on a wide range of sector-specific strategies, policies, and activities. The SRMAs and the SCCs coordinate and collaborate in a voluntary fashion on issues pertaining to their respective critical infrastructure sectors.

¹²Information Sharing and Analysis Centers are sector-based organizations with the purpose of maximizing information flow between private critical infrastructure entities and the government in order to better protect entities from cyber and physical security threats.

¹³We excluded financial services, communications, and the IT sectors. The SRMA for the financial services sector reported that IoT and OT are not used within the sector. In addition, SRMA for the communications and IT sector stated that although both sectors may use IoT and OT, these devices are not critical to their operations.

¹⁴William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283 § 9204, 134 Stat. 3388, 4797 (Jan. 1, 2021) (47 U.S.C. § 901 note).

¹⁵The White House, *Presidential Policy Directive 21: Critical Infrastructure Security and Resilience* (Washington, D.C.: Feb. 12, 2013).

NIST publications.¹⁶ We also met with industry representatives from the SCCs and ISACs for the respective sectors to obtain their perspectives on government efforts and on challenges with managing cybersecurity vulnerabilities associated with the use of IoT and OT devices.

To address the third objective, we obtained and described NIST and DHS guidance and best practices on the procurement of IoT devices. We also interviewed OMB officials to determine and describe the status of the waiver development process and steps to complete it.

For each of the objectives, we met with relevant agency officials to obtain their views and verify the information provided. For more information on our scope and methodology, see appendix I.

We conducted this performance audit from September 2021 to December 2022 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

IT, IoT, and OT devices and systems that support federal agencies and our nation's critical infrastructures are inherently at risk. These systems are highly complex, technologically diverse, and often geographically dispersed. In addition, they are often interconnected with other internal and external systems and networks, including the internet. This complexity increases the difficulty of identifying, managing, and protecting the numerous operating systems, applications, and devices comprising the systems and networks.

The risks facing these technologies include escalating and emerging threats from around the globe, the emergence of new and more destructive attacks, and insider threats from witting or unwitting employees. Recent incidents—such as the ransomware attack on the Colonial Pipeline and attacks targeting health care and essential services during the COVID-19 pandemic—illustrate the significant cyber threats

¹⁶National Institute of Standards and Technology, *IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements*, Special Publication 800-213 (Gaithersburg, MD: November 2021).

facing the nation's critical infrastructure and the range of consequences that these attacks pose.¹⁷

Due to the cyber-based threats to federal systems and critical infrastructure, the persistent nature of information security vulnerabilities, and the associated risks, we first designated federal information security as a government-wide high-risk area in our biennial report to Congress in 1997. In 2003, we expanded this high-risk area to include the protection of critical cyber infrastructure and, in 2015, we further expanded this area to include protecting the privacy of personally identifiable information. We continue to identify the protection of critical cyber infrastructure as a high-risk area, as shown in our March 2021 high-risk update on major cybersecurity challenges.¹⁸

Overview of IoT and OT

While there are a variety of definitions of IoT, the Internet of Things Cybersecurity Improvement Act of 2020¹⁹ describes IoT devices as having at least one transducer (sensor or actuator) for interacting directly with the physical world and one network interface, while not being

¹⁷On May 7, 2021, Colonial Pipeline, an American oil pipeline system that originates in Houston, Texas, and carries gasoline and jet fuel mainly to the Southeastern United States, suffered a ransomware cyberattack that impacted computerized equipment managing the pipeline. See GAO, [Colonial Pipeline Cyberattack Highlights Need for Better Federal and Private-Sector Preparedness \(infographic\)](#), (Washington, D.C.: May 18, 2021). In May 2020, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency released a joint alert with the United Kingdom's National Cyber Security Centre regarding advanced persistent threat groups exploiting COVID-19 to target health care and essential services. 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. See GAO, *HHS Defined Roles and Responsibilities, but Can Further Improve Collaboration*, [GAO-21-403](#) (Washington, D.C.: June 28, 2021).

¹⁸GAO, *High-Risk Series: Federal Government Needs to Urgently Pursue Critical Actions to Address Major Cybersecurity Challenges*, [GAO-21-288](#) (Washington, D.C.: Mar. 24, 2021).

¹⁹Internet of Things Cybersecurity Improvement Act of 2020, Pub. L. No. 116-207 § 2(4) (Sense of Congress), 134 Stat. 1001 (Dec. 4, 2020), 15 U.S.C. § 278g-3a note.

Internet of Things

conventional IT devices, such as smartphones and laptops.²⁰ Further, the definition notes that these devices can function on their own or as a component of another device, such as a processor. For example, a “connected” fitness tracker can monitor a user’s vital statistics, and transfer the information to a smartphone.

The act defines OT as hardware and software that detects or causes a change through the direct monitoring or control of physical devices, processes, and events.²¹ For example, OT systems can be required to control valves, engines, conveyors, and other machines to regulate various process values, such as temperature, pressure, flow, and to monitor them to prevent hazardous conditions.

According to NIST, IoT technology acts as a bridge between OT, which includes sensors and actuators, with IT, which includes data processing and networking. Every critical infrastructure sector has its own types of IoT, such as specialized connected hospital equipment in the healthcare and public health sector and smart road technologies in the transportation systems sector.

While the full scope of IoT is not precisely defined, it is clearly vast. NIST reported that IoT is a rapidly evolving and expanding collection of diverse digital technologies that interact with the physical world. Further, worldwide numbers of devices are predicted to increase to 43 billion by 2023.²²

Many IoT devices are the result of the convergence of cloud computing, mobile computing, embedded systems, big data, low-price hardware, and

²⁰According to NIST, transducer capabilities interact with the physical world and serve as the edge between digital and physical environments. They provide the ability for computing devices to interact directly with physical entities. Every IoT device has at least one transducer capability. The two types of transducer capabilities are: (1) sensing, which is the ability to provide an observation of an aspect of the physical world in the form of measurement data and (2) actuating, which is the ability to change something in the physical world. Examples of actuating capabilities include heating coils, cardiac electric shock delivery, electronic door locks, unmanned aerial vehicle operation, servo motors, and robotic arms. See also National Institute of Standards and Technology, *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks*, NISTIR 8228 (June 2019).

²¹Internet of Things Cybersecurity Improvement Act of 2020, Pub. L. No. 116-207 § 3(6), 134 Stat. 1001 -1002 (Dec. 4, 2020), 15 U.S.C. § 278g-3a.

²²McKinsey & Company, *Growing Opportunities in the Internet of Things* (July 2019) and [GAO-20-577](#).

other technological advances. IoT devices can provide computing functionality, data storage, and network connectivity for equipment that previously lacked them. This had enabled new efficiencies and technological capabilities for the equipment, such as remote access for monitoring, configuration, and troubleshooting. IoT can also add the abilities to analyze data about the physical world and use the results to better inform decision making, alter the physical environment, and anticipate future events.

Industrial Internet of Things (IIoT), a subset of the broader IoT, refers to the application of instrumentation and connected sensors and other devices to machinery and vehicles in the transportation systems, energy, and other critical infrastructure sectors. IIoT leverages many of the same technologies as IoT and applies them to industrial environments within critical infrastructure.²³ For example, these applications may include managing the flow of energy in the distribution grid in the energy sector.

Operational Technology

NIST describes OT as programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems and devices detect or cause a direct change through the monitoring or control of devices, processes, and events. Examples of OT include industrial control systems (ICS), Supervisory Control and Data Acquisition (SCADA) systems, and building automation systems, such as air conditioning, fire control systems, and physical access control mechanisms.

- ICS are found in many industries, such as electric, water and wastewater, oil and natural gas, chemical, pharmaceutical, pulp and paper, food and beverage, and discrete manufacturing (e.g., automotive, aerospace, and durable goods). These control systems consist of combinations of control components (e.g., electrical, mechanical, hydraulic, and pneumatic) that act together to achieve an industrial objective (e.g., manufacturing, transportation of matter or energy). Many of today's industrial control systems evolved from the insertion of IT capabilities into existing physical systems, often replacing or supplementing physical control mechanisms. Improvements in cost and performance have encouraged this evolution, resulting in many of today's "smart" technologies such as

²³National Institute of Standards and Technology, *Securing Distributed Energy Resources: An Example of Industrial Internet of Things Cybersecurity*, NIST Special Publication 1800-32 (February 2022).

the smart electric grid, smart transportation, smart buildings, and smart manufacturing.²⁴

- SCADA systems are used in distribution systems, such as water distribution and wastewater collection systems, oil and natural gas pipelines, electrical utility transmission and distribution systems, and rail and other public transportation systems. SCADA systems are designed to collect field information such as electricity distribution from utility companies, transfer it to a central computer facility, and display the information to the operator graphically or textually. This allows the operator to monitor or control an entire system from a central location in near real-time. Both the electrical power transmission and distribution grid industries use geographically distributed SCADA control technology to operate highly interconnected and dynamic systems consisting of thousands of public and private utilities and rural cooperatives for supplying electricity to end users.²⁵
- Building automation systems are a type of OT used to control many systems used in a building, including heating, ventilation, and air conditioning (HVAC), fire, electrical, lighting, physical access control, physical security, and other utility systems. Some of the most common functions of building automation systems are maintaining the environmental conditions for occupant comfort, reducing energy consumption, reducing operating and maintenance costs, increasing security, recording historical data (e.g., temperature, humidity), and performing general equipment monitoring (e.g., provide alerts to building personnel upon device failure or an alarm condition).

Traditional OT systems had little resemblance to traditional IT systems in that OT systems were isolated, ran proprietary control protocols, and used specialized hardware and software. As OT are designed to increasingly adopt IT solutions and implemented using industry-standard computers, operating systems, and network protocols, they are starting to resemble IT systems. This integration supports new IT capabilities, but it provides significantly less isolation for OT from the outside world than predecessor systems. This in turn creates a greater need to secure OT systems. The increasing use of wireless networking places OT implementations at greater risk from adversaries who are in relatively close physical proximity but do not have direct physical access to the

²⁴National Institute of Standards and Technology, *Guide to Industrial Control Systems (ICS) Security*, NIST Special Publication 800-82 Revision 2, (May 2015).

²⁵National Institute of Standards and Technology, *Guide to Industrial Control Systems (ICS) Security*, NIST Special Publication 800-82 Revision 2, (May 2015).

equipment. See figure 1 for an overview of the intersection between IT, IoT, and OT.

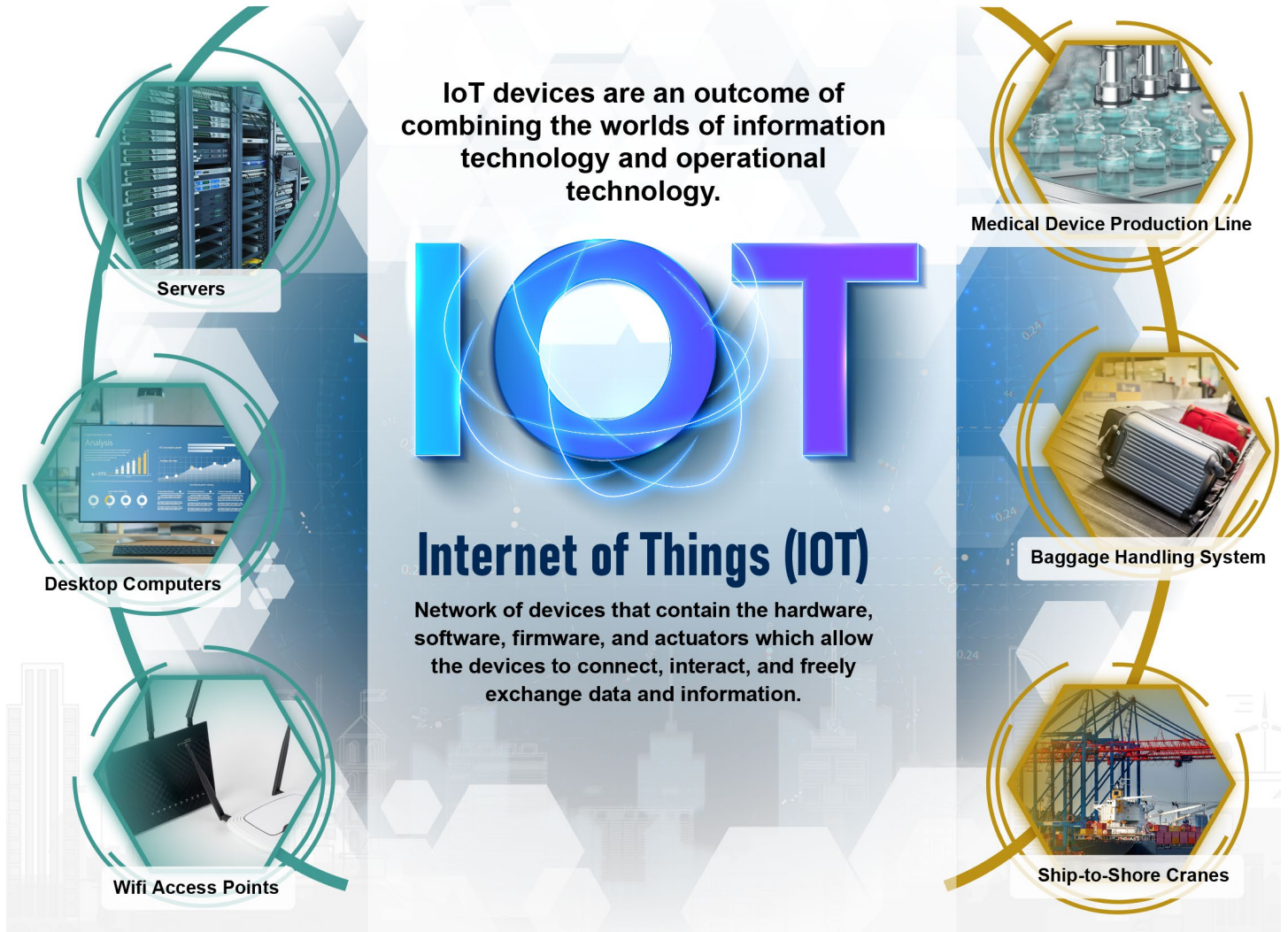
Figure 1: Intersection of IT, Internet of Things (IoT), and Operational Technology

INFORMATION TECHNOLOGY

Any equipment or interconnected system of equipment that can collect, store, process, maintain, share, transmit, or dispose of data.

OPERATIONAL TECHNOLOGY

Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment).



Source: GAO analysis of government and industry representative information; images: Zinetron/stock.adobe.com, wacomka/stock.adobe.com, Gorodenkoff/stock.adobe.com, patrikslezak/stock.adobe.com, Voy_ager/stock.adobe.com, .shock/stock.adobe.com, Александр Беспалый/stock.adobe.com. | GAO-23-105327

Cyber Threats to IoT and OT

IT, IoT, and OT devices and systems are subject to serious cyber threats that can have adverse impacts on organizational operations and assets, individuals, critical infrastructure, and the nation. As cyber threats grow increasingly sophisticated, the need to manage and bolster the cybersecurity of IoT and OT products and services is also magnified. These cyber threats can include purposeful attacks, environmental disruptions, and human/machine errors, and may result in harm to the national and economic security interests of the United States. Table 1 describes the types of cyberattacks that could affect IoT and OT devices and networks. Figure 2 depicts a theoretical botnet attack on the electric grid.

Table 1: Examples of Common and Damaging Types of Cyberattacks

Types of attack	Description
Botnet	A network of internet-connected computing devices infected with bot malware and that are remotely controlled by third parties for nefarious purposes. A botnet attack happens when a network of computers, Internet of Things, or other internet protocol-enabled devices are commandeered to run unauthorized code in support of malicious activities such as spam, ^a phishing, ^b and distributed denial of service (see below).
Data breach	An unauthorized or unintentional exposure, disclosure, or loss of an organization's sensitive information. This information can include personally identifiable information, such as Social Security numbers, or financial information, such as credit card numbers.
Denial-of-service	An attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources. A distributed denial-of-service attack is a variant of the denial-of-service attack that uses numerous hosts to perform the attack.
Malware	Also known as malicious code and malicious software, malware refers to a program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or otherwise annoying or disrupting the victim. Examples of malware include logic bombs, ^c Trojan Horses, ^d ransomware (see below), viruses, and worms. ^e
Man-in-the-middle	An attack where the attacker comes in between a two-party communication, i.e., the attacker hijacks the session between a client and host. By doing so, hackers steal and manipulate data.
Ransomware	A type of malware used to deny access to IT systems or data and hold the systems or data hostage until a ransom is paid.
Structured query language (SQL) injection	An attack that involves the alteration of a database search in a web-based application, which can be used to obtain unauthorized access to sensitive information in a database.
Zero-day exploit	An exploit that takes advantage of a security vulnerability previously unknown to the general public. In many cases, the exploit code is written by the same person who discovered the vulnerability. By writing an exploit for the previously unknown vulnerability, the attacker creates a potent threat since the compressed time frame between public discoveries of both makes it difficult to defend against.

Source: GAO analysis of DHS and NIST information and industry reports. | GAO-23-105327

^aSpam is electronic junk mail or the abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages.

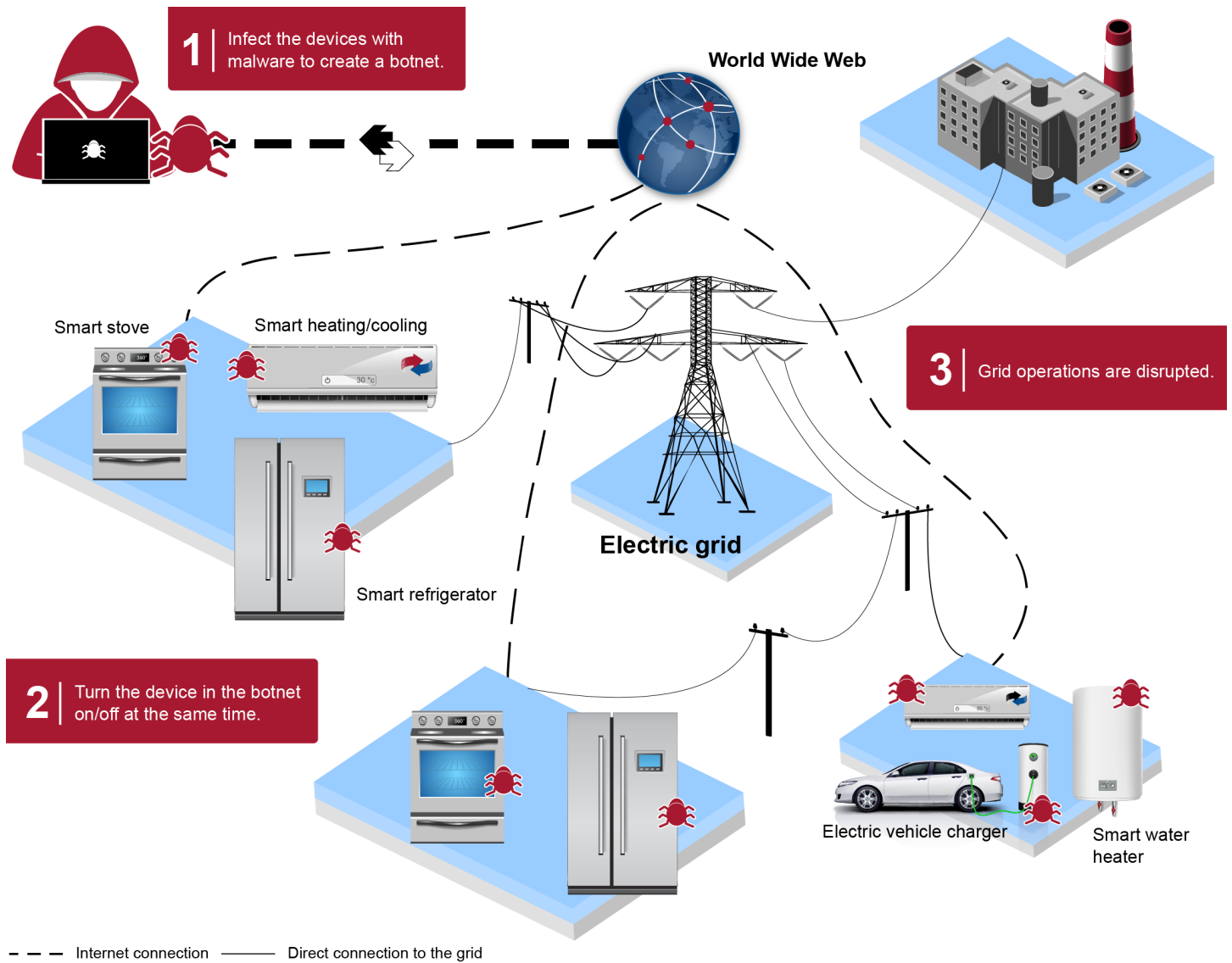
^bPhishing is a technique for attempting to acquire sensitive data, such as bank account numbers, through a fraudulent solicitation in email or on a web site, in which the perpetrator masquerades as a legitimate business or reputable person.

^cLogic bomb is a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met.

^dTrojan horse is a computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program.

^eWorms are computer programs that can run independently, can propagate a complete working version of itself onto other hosts on a network, and may consume computer resources destructively.

Figure 2: Theoretical Depiction of a Botnet Attack on the Electrical Grid



Sources: GAO and university research; images left to right: ifh85/stock.adobe.com, sveta/stock.adobe.com, and mark.f/stock.adobe.com. | GAO-23-105327

Cybersecurity incidents, including those targeting IoT and OT devices and systems, continue to impact federal agencies, as well as entities across various critical infrastructure sectors. In 2021, the Federal Bureau of

Investigation's Internet Crime Complaint Center²⁶ received 649 complaints that indicated organizations belonging to a critical infrastructure sector were victims of a ransomware attack.²⁷ Of the 16 critical infrastructure sectors, the center indicated 14 sectors had at least one member that reported falling victim to a ransomware attack in 2021. Recent events highlight the significant IoT and OT cyber threats facing the nation and the range of consequences that these attacks pose.

- In June 2022, the Department of Justice reported that a Russian botnet targeted a broad range of IoT and OT devices. These devices included time clocks, routers, audio/video streaming devices, smart garage door openers, and ICSs, which are connected to and can communicate over the internet. Millions of devices were compromised, and victims varied from large entities—including a university, hotel, television studio, and electronic manufacturers—to private entities such as home businesses and individuals.²⁸
- In July 2022, a joint alert from CISA, the Department of the Treasury, and the Federal Bureau of Investigation stated that a North Korean ransomware attack targeted the healthcare and public health sector organizations. Specifically, the alert identified electronic health records services, diagnostics services, imaging services, and intranet services as targets. The agencies urged the sector organizations to limit access to data with authenticated connections to the network, IoT medical devices, and the electronic health record systems to ensure data packages were not manipulated while in transit.²⁹

²⁶The Federal Bureau of Investigation's Internet Crime Complaint Center was established in May 2000 to receive complaints of internet related crime and has received more than 6.5 million complaints since its inception. Its mission is to provide the public with a reliable and convenient reporting mechanism to submit information to the Bureau concerning suspected cyber enabled criminal activity, and to develop effective alliances with law enforcement and industry partners to help those who report.

²⁷Federal Bureau of Investigation, *2021 Internet Crime Report*, (2021).

²⁸Department of Justice U.S Attorney's Office Southern District of California, "Russian Botnet Disrupted in International Cyber Operations" (San Diego, California, June 16, 2022), accessed August 3, 2022, <https://www.justice.gov/usao-sdca/pr/russian-botnet-disrupted-international-cyber-operation>.

²⁹Cybersecurity and Infrastructure Security Agency, Alert (AA22-187A) "North Korean State-Sponsored Cyber Actors Use Maui Ransomware to Target the Healthcare and Public Health Sector" (July 7, 2022), accessed Aug. 3, 2022, <https://www.cisa.gov/uscert/ncas/alerts/aa22-187a>.

Federal Roles and Responsibilities for Adoption and Use of IoT and OT

Several entities within the federal government have responsibilities for helping oversee and guide the adoption and use of IoT and OT technologies.

OMB. The agency oversees the management of federal agencies' IT and, in conjunction with other agencies, implements the President's Management Agenda, which emphasizes the importance of IT modernization, as well as data, accountability, and transparency, among other things. According to OMB, its role and the role of the Office of the Federal Chief Information Officer are to enable agencies to adopt IT technology, including IoT, just as they would any other IT technology, in a manner that is consistent with the President's budget and that enhances the agency's mission.³⁰ OMB also noted that it encourages the adoption of best practices in IT that mitigate cyber risk arising from IoT or other operations.

DHS. The agency oversees IT-specific issues in support of the 2013 National Infrastructure Protection Plan (referred to as the National Plan).³¹ In this role, DHS coordinates with other federal agencies, works with private sector entities that support IT infrastructure, and contributes to the development of guidance related to security considerations when acquiring IoT devices. In addition, the Federal Information Security Modernization Act of 2014 authorized DHS to issue binding operational directives that align with policies, principles, standards, and guidelines.³² These directives require agencies to safeguard federal information and information systems from a known or reasonable suspected information security threat, vulnerability, or risk including IoT and OT devices.

³⁰The Federal Chief Information Officer is the presidential designation for the Administrator of the OMB Office of Electronic Government and Information Technology, which was created by the E-Government Act of 2002. Pub. L. No. 107-347, 116 Stat. 2899 (Dec. 17, 2002).

³¹Department of Homeland Security, *National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience* (Washington, D.C.: December 2013). The *National Plan* outlines how government and private sector participants in the critical infrastructure community can work together to manage risks and achieve security and resilience outcomes for their information systems. To achieve this end, critical infrastructure partners must collectively identify national priorities, articulate clear goals, mitigate risk, measure progress, and adapt based on feedback and the changing environment.

³²Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283 § 2 (44 U.S.C. § 3553(b)(2)), 128 Stat. 3073, 3076 (Dec. 18, 2014).

In addition, the Cybersecurity and Infrastructure Security Agency Act of 2018 established CISA within DHS.³³ As implemented, CISA is responsible for developing and implementing information sharing programs through which it develops partnerships and shares substantive information with the private sector, and state, local, tribal, and territorial governments, to include information on IoT and OT threats. In addition to information sharing initiatives, CISA is also responsible for developing resources to help spread awareness about cyber threats, protective measures, and response tactics.

NIST. The agency conducts research and develops standards, guidelines, and tools for public and non-public organizations. NIST develops security standards and guidelines for non-national security federal agency systems, which can be mandatory for federal agencies. NIST has issued multiple publications and engaged in projects to help manage the security of IoT and OT such as Special Publication *IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements*, which is intended to help organizations securely incorporate IoT devices into an existing information system as system elements.³⁴

Federal Acquisition Regulatory Council. The Federal Acquisition Regulation (FAR) is the primary regulation used by all federal executive agencies to acquire supplies and services with appropriated funds. The council, which consists of the Secretary of Defense and the Administrators of the Office of Federal Procurement Policy in OMB, NASA, and GSA, assists in the direction and coordination of government-wide procurement policy and regulatory activities. The council is responsible for maintaining the FAR and managing, coordinating, and controlling changes in the FAR. Several revisions to the FAR, as discussed later, are being considered based on recent NIST guidance on IoT and OT cybersecurity, among other things.

³³The Cybersecurity and Infrastructure Security Agency Act of 2018, Pub. L. No. 115-278 § 2, 132 Stat. 4168, 4169 (Nov. 16, 2018), adding sec. 2202 to the Homeland Security Act of 2002, 6 U.S.C. § 652.

³⁴National Institute of Standards and Technology, *IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements*, Special Publication 800-213 (Gaithersburg, MD: November 2021).

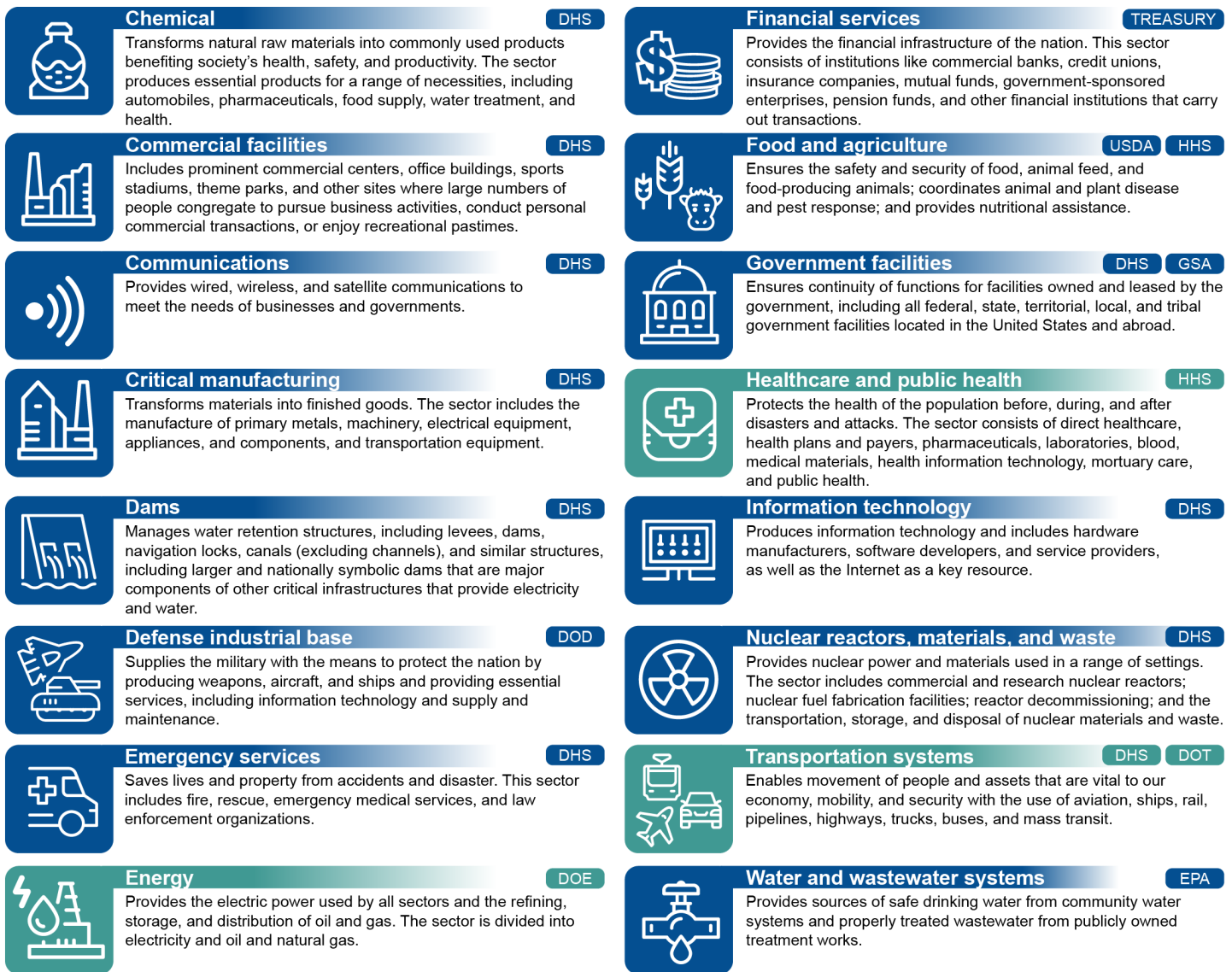
Critical Infrastructure Sectors' Roles and Responsibilities

Presidential Policy Directive 21³⁵ identified 16 critical infrastructure sectors and designated the SRMAs. Subsequently, section 9002 of the FY2021 NDAA³⁶ established roles and responsibilities for the SRMAs in protecting their critical infrastructure sectors. Figure 3 illustrates these 16 sectors and each sector's SRMA.

³⁵The White House, *Presidential Policy Directive 21: Critical Infrastructure Security and Resilience* (Washington, D.C.: Feb. 12, 2013).

³⁶William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283 § 9002, 134 Stat. 3388, 4768 (Jan. 1, 2021), 6 U.S.C. § 652a.

Figure 3: Critical Infrastructure Sectors and Related Sector Risk Management Agencies



Sector Risk Management Agency

 Reflects the three selected sectors in this report. **USDA** (Department of Agriculture), **DOD** (Department of Defense), **DOE** (Department of Energy), **HHS** (Department of Health and Human Services), **DHS** (Department of Homeland Security), **DOT** (Department of Transportation), **Treasury** (Department of the Treasury), **EPA** (Environmental Protection Agency), **GSA** (General Services Administration).^a

Source: GAO analysis of Presidential Policy Directive-21 and DHS's National Infrastructure Protection Plan 2013; images: motorama/stock.adobe.com. | GAO-23-105327

^aFive of the nine SRMAs—DHS, DOT, GSA, HHS, and Agriculture—also function as co-SRMAs, in which they work collaboratively to support a particular sector. Specifically, as co-SRMAs, HHS and Agriculture lead the food and agriculture sector; GSA and DHS lead the government facilities sector; and DHS and DOT lead the transportation systems sector.

Selected Critical Infrastructure Sectors' IoT and OT Environments

For the three sectors we selected (energy, healthcare and public health, and transportation systems), the SRMAs and SCC and ISAC industry representatives described varied environments and uses of IoT and OT. Tables 2 and 3 below describe each sector's IoT and OT environments.

Table 2: Selected Critical Infrastructure Sectors' Internet of Things (IoT) Environment

Sector	IoT activities
Energy	Department of Energy officials and representatives from the oil & natural gas subsector stated that IoT is not widely used as part of their critical functions. ^a The electricity subsector noted that IoT-type devices used by utilities might be considered internet-connected operational technology (OT). ^b
Healthcare and public health	Department of Health and Human Services and Food and Drug Administration officials as well as health care and public health representatives stated that IoT includes network-connected medical devices ^c as part of their critical functions for sector operations.
Transportation systems	<p>As co-Sector Risk Management Agencies (SRMA) for the sector, the Department of Homeland Security (the Transportation Security Administration and the U.S. Coast Guard) and Department of Transportation officials stated that the use of IoT varies and they do not know the extent to which IoT devices are used in the selected subsectors. However, representatives for the selected subsectors reported the following types of possible IoT and Industrial Internet of Things (IIoT):^d</p> <ul style="list-style-type: none"> • Aviation—IoT uses include access controls, badge readers, elevator readers, and video equipment for security systems. • Maritime Transportation Systems—IoT usage varies depending on the port, company, and type of operations. IIoT devices used for management of data such as providing efficiency for fuel usage and monitoring routes or cranes. • Mass Transit and Passenger Rail—IoT applications include advising passengers when the next bus or train is arriving to their locations.

Source: GAO analysis of selected SRMA and industry representatives' information. | GAO-23-105327

^aIn 2019, CISA published an initial set of 55 National Critical Functions, which are the functions of governmental and nongovernmental entities so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof. By viewing risk through a functional lens, the critical infrastructure community can identify where key dependencies and interdependencies lie between cyber and physical systems, as well as between National Critical Functions. For example, if the electric grid is knocked offline, water and wastewater systems cannot provide clean water, natural gas cannot flow to provide heat, and telecommunications systems may become inoperative if backup power sources fail.

^bInternet-connected OT or Industrial Internet of Things would include distributed energy resources, such as solar photovoltaics including sensors, data transfer and communications systems, instruments, and other commercially available devices that are networked together.

^cIoT medical devices could include the workstations controlling diagnostic and interventional imaging machines or the servers dedicated to patient monitoring systems. For example, an infusion pump to deliver fluids to patients, blood pressure monitoring, Magnetic Resonance Imaging, and patient bedside monitoring for diagnostic and therapeutic purposes for a patient's state of care. In addition to IoT medical devices located in medical settings and control(able) by a provider facility, an additional subset of such devices includes individual patient devices such as patient-implanted insulin pumps and pacemakers, as well as other medical devices that a patient uses at home.

^dIIoT, a subset of the broader IoT, refers to the application of instrumentation and connected sensors and other devices to machinery and vehicles in the transport, energy, and other critical infrastructure sectors.

Table 3: Selected Critical Infrastructure Sectors' Operational Technology (OT) Environment

Sector	OT activities
Energy	Department of Energy officials and representatives from the oil & natural gas subsector stated that OT comprises the majority of the technology used for critical functions for sector operations, such as substations, generating stations and industrial control systems. ^a Further, there are many activities associated with the cybersecurity of grid technologies, which officials typically consider to be OT, including smart-technologies.
Healthcare and public health	Department of Health and Human Services and Food and Drug Administration (FDA) officials as well as industry representatives stated that OT is primarily found in the physical healthcare delivery environment and on production lines of medical device and pharmaceutical manufacturers, as well such areas as building management and mortuary equipment, FDA efforts are primarily focused on medical devices.
Transportation systems	<p>As co-Sector Risk Management Agencies (SRMA) for the sector, the Department of Homeland Security (DHS) and Department of Transportation officials stated that they do not have a comprehensive understanding of OT devices across the subsectors. However, officials from DHS's Transportation Security Administration and the U.S. Coast Guard stated they are aware that some subsector applications rely specifically on OT, such as within the pipeline systems subsector and the maritime transportation systems subsector. Representatives for the selected subsectors reported the following types of possible OT:</p> <p>Aviation—baggage handling systems and air conditioning for various facilities.</p> <p>Maritime Transportation Systems—engines, ballast, bilge water and control systems that function on the mechanics of a vessel, systems for steering, monitoring, powering vessels, automated systems such as GPS, radar, and electronic chart displays, and ship-to-shore cranes or rubber tire gantry cranes.</p> <p>Mass Transit and Passenger Rail—Supervisory Control and Data Acquisition (SCADA) devices to control the speed of trains, signals and gates, and other signaling devices^b as well as OT devices for roadways, lighting systems, heating, and ventilation systems.</p>

Source: GAO analysis of selected SRMA and industry representatives' information. | GAO-23-105327

^aIndustrial control systems consist of combinations of control components (e.g., electrical, mechanical, hydraulic, and pneumatic) that act together to achieve an industrial objective (e.g., manufacturing, transportation of matter or energy).

^bSCADA systems are designed to collect field information, transfer it to a central computer facility, and display the information to the operator graphically or textually, thereby allowing the operator to monitor or control an entire system from a central location in near real time.

GAO Has Previously Reported on the Status of IoT and Cybersecurity Risks Facing Critical Infrastructure Sectors

In May 2017, we reported on the status and implications of IoT. The report provided an introduction to IoT and described what was known about current and emerging IoT technologies, and the implications of their use. We reported that while the rapid emergence of IoT brings the promise of important new benefits, it also presents potential challenges, including security risks.³⁷

Subsequently, in July of 2017, we reported that although the Department of Defense had begun to examine security risks of IoT devices through its

³⁷GAO, *Internet of Things: Status and Implications of an Increasingly Connected World*, GAO-17-75 (Washington D.C.: May 15, 2017).

infrastructure-related and intelligence assessments, it had not conducted required assessments related to the security of its operations. We noted that risks with IoT devices included risks with the devices themselves, (limited encryption and a limited ability to patch or upgrade devices), and operational risks or how they are used (insider threats and unauthorized communication). We also noted that the department had issued policies and guidance for IoT devices, including personal wearable fitness devices, portable electronic devices, smartphones, and infrastructure devices associated with industrial control systems. However, we found that these policies and guidance did not clearly address some security risks relating to IoT devices. Accordingly, we made two recommendations that Defense has since implemented.³⁸

Additionally, in August 2020, we reported that many federal agencies used IoT technologies for a variety of purposes, such as to control or monitor equipment or systems and to control access to devices or facilities. We also noted that agencies often identified increased data collection and operational efficiencies as benefits and cybersecurity and interoperability as challenges.³⁹

We have also conducted numerous reviews of critical infrastructure sectors looking at, among other things, adoption of cybersecurity guidance,⁴⁰ cybersecurity risks facing the electric grid,⁴¹ oversight of avionics risks,⁴² passenger rail security,⁴³ and medical device information

³⁸GAO, *Internet of Things: Enhanced Assessments and Guidance Are Needed to Address Security Risks in DOD*, [GAO-17-668](#) (Washington, D.C.: July 27, 2017).

³⁹[GAO-20-577](#).

⁴⁰GAO, *Critical Infrastructure Protection: Agencies Need to Assess Adoption of Cybersecurity Guidance*, [GAO-22-105103](#) (Washington, D.C.: Feb. 9, 2022).

⁴¹GAO, *Electricity Grid Cybersecurity: DOE Needs to Ensure Its Plans Fully Address Risks to Distribution Systems*, [GAO-21-81](#) (Washington, D.C.: Mar. 18, 2021), and *Critical Infrastructure Protection: Actions Needed to Address Significant Cybersecurity Risks Facing the Electric Grid*, [GAO-19-332](#) (Washington, D.C.: Aug. 26, 2019).

⁴²GAO, *Aviation Cybersecurity: FAA Should Fully Implement Key Practices to Strengthen Its Oversight of Avionics Risks*, [GAO-21-86](#) (Washington, D.C.: Oct. 9, 2020).

⁴³GAO, *Passenger Rail Security: TSA Engages with Stakeholders but Could Better Identify and Share Standards and Key Practices*, [GAO-20-404](#) (Washington, D.C.: Apr. 3, 2020).

security considerations.⁴⁴ For example, in February 2022, we reported that most of the agencies with a lead role in protecting the 16 critical infrastructure sectors had not developed methods to determine the level and type of adoption of the NIST Framework for Improving Critical Infrastructure Cybersecurity (framework). In addition, we acknowledged that challenges associated with the difficulty of developing precise measurements of improvement given the voluntary nature of the framework adoption exist. We noted that despite these challenges, several SRMAs had successfully determined framework adoption for their sectors or were taking steps to do so.⁴⁵

Federal agencies have not implemented most of our recommendations related to the challenge of protecting critical infrastructure. Of the over 90 recommendations made in our public reports since 2010, over 50 had not been implemented as of June 2022. We have also designated 14 as priority recommendations, and as of June 2022, 10 had not been implemented. Until our recommendations are fully implemented, federal agencies may be limited in their ability to ensure the critical infrastructures are protected from potentially harmful cybersecurity threats.

We have also reported on CISA's coordination with stakeholders.⁴⁶ Specifically, in March 2021, we reported that selected government and private-sector stakeholders from the 16 sectors considered to be critical infrastructures, such as banking and financial institutions, telecommunications, and energy, reported a number of challenges in coordinating with CISA. These challenges included a lack of timely responses and inconsistent distribution of information. We noted that CISA had activities under way to mitigate some of these challenges, including tracking stakeholder inquiries to monitor the timeliness of responses and delivering briefings with intelligence tailored to stakeholder needs. However, we reported that CISA had not developed strategies to have consistent stakeholder involvement in the development of guidance, and distribute information to all key stakeholders. Accordingly, we recommended that CISA collect input to ensure that organizational

⁴⁴GAO, *Medical Devices: FDA Should Expand Its Consideration of Information Security for Certain Types of Devices*, [GAO-12-816](#) (Washington, D.C.: Aug. 12, 2012).

⁴⁵[GAO-22-105103](#).

⁴⁶GAO, *Cybersecurity and Infrastructure Agency: Actions Needed to Ensure Organizational Changes Result in More Effective Cybersecurity for Our Nation*, [GAO-21-236](#) (Washington, D.C.: Mar. 10, 2021).

changes are aligned with the needs of stakeholders, taking into account coordination challenges identified in this report.

CISA concurred with this recommendation and in September 2021 stated that it will continue to work with other SRMAs and with sector partners to define measures and associated data collection processes and procedures necessary to evaluate the effectiveness and performance of SRMAs. This will include the extent to which organizational changes within CISA, or any other SRMA, are aligned with the needs of sector stakeholders. CISA plans to complete this effort by December 30, 2022.

Federal Agencies Have Issued Guidance for Managing IoT and OT Cybersecurity Risks

CISA and NIST have issued guidance and provided resources to help agencies and private entities manage cybersecurity risks associated with the use of IoT and OT devices. In addition, the FAR Council is considering updates to current guidance on IoT and OT cybersecurity.

CISA Established Programs and Directives on IoT and OT Cybersecurity

CISA has several programs and directives intended to help manage cybersecurity risks to federal information systems and critical infrastructure that include, as appropriate, IoT and OT. CISA officials stated that they generally consider IoT to be a component of IT overall, and do not track information on the extent of IoT and OT use in individual critical infrastructure sectors.

Coordinated Vulnerability Disclosure Program. This program coordinates the remediation and public disclosure of newly identified cybersecurity vulnerabilities in products and services with the affected vendor(s). This includes new vulnerabilities in OT, such as in ICS, as well as IoT and traditional IT vulnerabilities. Officials noted that in CISA's national coordinated disclosure program, IoT vulnerabilities are not differentiated from vulnerabilities in other IT and are treated the same.

Binding Operational Directives. As noted earlier, these directives require agencies to safeguard federal information and information systems—including IoT and OT, as appropriate—from a known or reasonably suspected information security threat, vulnerability, or risk. For

example, in November 2021, Binding Operational Directive 22-01⁴⁷ established a CISA-managed catalog of known exploited vulnerabilities that carry significant risk to the federal enterprise, including vulnerabilities in IoT devices and requirements for agencies to remediate any such vulnerabilities included in the catalog.⁴⁸ Further, in October 2022, CISA issued Binding Operational Directive 23-01, which requires all federal civilian executive branch agencies to maintain an up-to-date inventory of networked assets; and identify software vulnerabilities.⁴⁹

In addition, CISA has resources intended to help agencies and organizations with managing cybersecurity risk associated with IoT and OT devices. For example, CISA's United States Computer Emergency Readiness Team (US-CERT)⁵⁰ and ICS Cyber Emergency Response Team (ICS-CERT)⁵¹ offer multiple resources to organizations that use IoT and OT, including alerts and advisories on specific cybersecurity vulnerabilities affecting IoT and OT devices. See table 4 for a list of CISA publications on IoT cybersecurity.

⁴⁷Department of Homeland Security, *Binding Operational Directive 22-01: Reducing the Significant Risk of Known Exploited Vulnerabilities* (Nov. 3, 2021), online at <https://www.cisa.gov/binding-operational-directive-22-01>.

⁴⁸The catalog is published at <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>.

⁴⁹Department of Homeland Security, *Binding Operational Directive 23-01: Improving Asset Visibility and Vulnerability Detection on Federal Networks* (Oct. 3, 2022), online at <https://www.cisa.gov/binding-operational-directive-23-01>.

⁵⁰CISA's US-CERT is responsible for leading efforts to improve the nation's cybersecurity posture, coordinate cyber information sharing, and proactively manage cyber risks to the government and private sector.

⁵¹The ICS-CERT is responsible for taking steps to reduce risk to the nation's critical infrastructure by strengthening control systems security and resilience through public-private partnerships. In executing its mission, ICS-CERT is to serve its partners as the preeminent federal government resource for industrial control systems security. Industrial control systems are also a form of operational technology.

Table 4: Selected Cybersecurity and Infrastructure Security Agency (CISA) Internet of Things (IoT) Cybersecurity Publications

Publication	Description
<i>United States Computer Emergency Readiness Team Security Tip ST17-001, Securing the Internet of Things.</i> (November 2019).	Intended to provide tips for improving the security of internet-enabled IoT devices, such as ensuring software is up-to-date and using strong passwords. ^a
<i>CISA’s Cybersecurity and Physical Security Convergence.</i> (January 2021)	Intended to describe the risks associated with siloed security functions within organizations, a description of how organizations can benefit from converging their security functions, a flexible framework for aligning security functions, and several case studies. ^b Notes that the adoption and integration of IoT and Industrial IoT devices have led to an increasingly interconnected mesh of cyber-physical systems, which expands the attack surface and blurs the distinction between cybersecurity and physical security.
<i>IoT Security Acquisition Guidance for the IT Sector.</i> (February 2020)	Intended to highlight areas of elevated risk resulting from the software-enabled and connected aspects of IoT technologies and their role in the physical world. Provides information on certain vulnerabilities and weaknesses, suggests solutions for common challenges, and identifies factors to consider before purchasing or using IoT devices, systems, and services. Designed to improve the effectiveness of supply chain, vendor, and technology evaluations prior to the purchase of IoT devices, systems, and services. ^c

Source: GAO summary of CISA publications. | GAO-23-105327

^aCybersecurity and Infrastructure Security Agency, *Securing the Internet of Things, Security Tip (17-001)*, Original release date: November 16, 2017 | Last revised: Nov. 14, 2019, available online at <https://www.cisa.gov/uscert/ncas/tips/ST17-001>.

^bCybersecurity and Infrastructure Security Agency, *Cybersecurity and Physical Security Convergence*, (January 2021), available online at <https://www.cisa.gov/publication/cybersecurity-and-physical-security-convergence>.

^cCybersecurity and Infrastructure Security Agency, *Internet of Things Security Acquisition Guidance: IT Sector* (February 2020). CISA, and the General Services Administration and the IT sector coordinating council collaboratively developed the guidance. According to administration officials, the guidance is applicable to any critical infrastructure sector.

In addition to online and in-person training on OT cybersecurity specific to industrial control systems, CISA offers other resources for OT cybersecurity, such as threat alerts and guidance. See table 5 for a list of CISA publications on OT cybersecurity.

Table 5: Selected Cybersecurity and Infrastructure Security Agency (CISA) Operational Technology (OT) Cybersecurity Publications

Publication	Description
<i>Advanced Persistent Threats (APT) Targeting Industrial Control Systems (ICS)/Supervisory control and data acquisition (SCADA) Advisory.</i> (April 2022)	<p>Advised organizations that certain advanced persistent threat actors have shown the capability to gain full system access to multiple ICS/SCADA devices.</p> <p>Recommended that agencies take several actions to mitigate the threat, such as isolating ICS/SCADA systems using strong perimeter controls, enforcing multifactor authentication whenever possible, and limiting network connections to only specifically allowed management and engineering workstations.^a</p> <p>Issued jointly by CISA, the Department of Energy, the National Security Agency, and the Federal Bureau of Investigation as part of the Department of Homeland Security’s Shields Up initiative.^b</p>
<i>Mitigating Attacks Against Uninterruptible Power Supply Devices.</i> (March 2022)	<p>Advised organizations to take certain actions to mitigate attacks against internet-connected uninterruptible power supply devices.^c</p> <p>Recommended that organizations ensure that these devices and similar systems are not internet accessible and change factory default login credentials, among other things.</p> <p>Issued jointly by CISA and the Department of Energy.</p>
<i>Recommended Cybersecurity Practices for Industrial Control Systems.</i> (May 2020)	<p>Outlines actions that ICS operators may take to protect these systems from cyberattacks, as well as steps they should consider to ensure better cybersecurity over ICS in the future.</p> <p>Issued by CISA and the Department of Energy.</p>
<i>Critical Infrastructure: Get Your Stuff Off Search.</i> (February 2022)	<p>Advised actions that owners and operators of Industrial Internet of Things devices, SCADA systems, and ICS can take to reduce their risk exposure from having searchable, internet-connected devices on their networks.^d</p> <p>Issued by CISA.</p>
<i>Control System Defense: Know the Opponent, Alert AA22-265A,</i> (September 2022)	<p>Advised owners and operators on the methods potential attackers use to target ICS.</p> <p>Provided recommendations on how to reduce malicious activity and reduce risk exposure of OT assets, including by limiting exposure of system information and identifying and securing remote access points.</p> <p>Issued jointly by CISA and the National Security Agency.</p>

Source: GAO summary of DHS publications. | GAO-23-105327

^aCybersecurity and Infrastructure Security Agency, “APT Cyber Tools Targeting ICS/SCADA Devices” (Apr. 13, 2022) accessed July 11, 2022, <https://www.cisa.gov/uscert/ncas/alerts/aa22-103a>.

^bCISA initiated the Shields Up initiative to help organizations prepare for, respond to, and mitigate the impact of cyberattacks in response to the increased cyber threat posed by Russia as a result of economic sanctions imposed on Russia following that country’s invasion of Ukraine.

^cAccording to NIST, an uninterruptible power supply is a device with an internal battery that allows connected devices to run for at least a short time when the primary power source is lost.

^dCybersecurity and Infrastructure Security Agency, “Get Your Stuff Off Search,” accessed Sept. 20, 2022, <https://www.cisa.gov/publication/stuff-off-search>.

In addition to publications and guidance, DHS has several working groups on OT and offers vulnerability assessments to public and private sector stakeholders.

ICS Joint Working Group. In 2009, DHS established the ICS Joint Working Group to help reduce cyber risk to the nation’s industrial control

systems by facilitating partnerships in all 16 critical infrastructure sectors between federal, state, and local governments; asset owners and operators; and vendors, among others. Among other things, the working group sponsors biannual meetings that allow stakeholders to gather and exchange ideas as well as to learn about critical cybersecurity issues in ICS. The working group also publishes a quarterly newsletter with information on upcoming meetings, events, trainings, technology, and other items related to ICS security.

Joint Cyber Defense Collaborative. In August 2021, CISA founded the organization as a public-private sector partnership, including many industry partners from multiple critical infrastructure sectors. The organization is intended to drive cybersecurity collaboration across sectors. In April 2022, CISA expanded the Joint Cyber Defense Collaborative to include OT, specifically including companies with ICS expertise.

CyberSentry. CISA officials noted that this CISA-managed threat detection and monitoring platform is intended to help gain operational visibility of critical IT and OT networks within the critical infrastructure sectors and identify and defend against cyber risks and incidents. The platform is also intended to monitor networks for novel and known malicious activity affecting critical infrastructure participants, and is intended to provide three key enhancements: (1) improve historical and current cyber situational awareness for sector entities and CISA; (2) enable CISA to analyze incidents across sectors to identify commonalities and trends; and (3) provide CISA with operational insights to inform protection of the larger critical infrastructure community and federal assets.

CISA Cyber Assessments. CISA officials provided a list of eight different cyber assessment options offered for public and private sector stakeholders, such as a risk and vulnerability assessment⁵² and a

⁵²Risk and vulnerability assessment is a service in which the assessor uses a number of techniques to identify weaknesses in the security posture of a given high value asset. These techniques can include network mapping, vulnerability scanning, phishing tests, wireless assessments, web application assessments, and database assessments.

validated architecture design review⁵³ that entities can request. Officials added that these assessments are not targeted at any one sector, are ubiquitous across all sectors, and are not specific to IoT or OT. Additionally, officials stated CISA balances its limited resources to perform these services. CISA reported that from fiscal year 2019 to fiscal year 2022, 79 validated architecture reviews were conducted for the three selected sectors (see table 6). Further, CISA officials reported there are 154 open requests for validated architecture reviews from the three selected sectors.

Table 6: Validated Architecture Design Reviews by Sector and Fiscal Year (FY)

	Energy	Healthcare and public health	Transportation systems	Total (by FY)
FY 2022	2	0	1	3
FY 2021	42	4	6	52
FY 2020	3	1	8	12
FY 2019	10	0	2	12
Total (by sector)	57	5	17	79

Source: Cybersecurity and Infrastructure Security Agency. | GAO-23-105327

The President’s National Security Telecommunications Advisory Committee (NSTAC). The NSTAC is a presidential advisory committee governed by the Federal Advisory Committee Act, and administered by DHS. The NSTAC provides industry-based analyses and recommendations to the Executive Office of the President on how the government can enact policy for, or take actions to enhance, national security and emergency preparedness telecommunications. In May 2021, in the aftermath of a series of significant cybersecurity incidents, the White House tasked the committee with conducting a multi-phase study on “Enhancing Internet Resilience in 2021 and Beyond.” The tasking directed the committee to focus on, among other things, the convergence of IT and OT.

⁵³CISA’s Validated Architecture Design Review encompasses architecture and design review, system configuration, log file review, and analysis of network traffic to develop a detailed representation of the communications, flows, and relationships between devices in order to identify anomalous communication flows. Reviews are based on standards, guidelines, and best practices and are designed for operational technology and information technology environments. After the review, the organization receives an in-depth report that includes findings and recommendations for improving operations and cybersecurity.

In August 2022, the committee submitted a draft report to the President on security issues associated with IT and OT convergence. According to the report, it aimed to identify opportunities for the federal government to aid in a secure convergence of OT cybersecurity within all relevant stakeholder communities. The report concluded that there needs to be a stronger understanding of the relationship between cybersecurity for converging OT systems and organizational mission and risk. It highlighted several recommendations in this regard that we describe later. As of August 2022, a timeline for the final report was not yet available.⁵⁴

In 2014, the National Security Council tasked the committee to examine the cybersecurity implications of the IoT within the context of national security and emergency preparedness. In November 2014, the committee issued its report, in which it found, among other things, that

- the cybersecurity implications related to IoT are enormous;
- the massive deployment of IoT devices as part of interconnected ecosystems, including consumer and national security systems, is driving the need to adjust cybersecurity policies to cover, respond, detect, and protect;
- IoT represents a convergence, or perhaps a collision, of IT and OT; and
- IoT is not addressed in a number of national cybersecurity strategic guidance documents; thereby, leaving roles, responsibilities, authorities and resourcing unclear relative to maximizing benefit and minimizing risk associated with IoT.⁵⁵

The report concluded that existing governance, policy, and institutional support structures are not well-equipped to facilitate the rapid changes needed and made several recommendations in this regard.

NIST Undertook Efforts for Managing Cybersecurity Risks to IoT and OT

NIST has several efforts intended to help manage cybersecurity risks to federal information systems and critical infrastructure that include, as appropriate, IoT and OT. These include publications, a center of

⁵⁴The President's National Security Telecommunications Advisory Committee (NSTAC), *Draft NSTAC Report to the President: Information Technology and Operational Technology Convergence* (August 2022).

⁵⁵National Security Telecommunications Advisory Committee (NSTAC), *NSTAC Report to the President: Report to the President on the Internet of Things* (Nov. 19, 2014).

excellence, working groups, and labeling programs for consumer IoT products.

NIST Publications

The Internet of Things Cybersecurity Improvement Act of 2020 requires NIST to develop and publish guidance on minimum information security standards for IoT devices that U.S. government agencies procure.⁵⁶ To fulfill its requirements, NIST has issued a number of publications intended to help federal agencies manage cybersecurity risks associated with the use of IoT devices. Specifically, NIST issued Special Publications including *IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements* and *IoT Device Cybersecurity Guidance for the Federal Government: IoT Device Cybersecurity Requirement Catalog* in November 2021.⁵⁷

The agency has also issued several publications through its Cybersecurity for the IoT Program.⁵⁸ In addition, it has also issued several publications on aspects of IoT cybersecurity, such as information about applying certain baseline cybersecurity recommendations to IoT in an organization's environment.⁵⁹ Table 7 describes key NIST publications for IoT cybersecurity. Further, appendix II includes a list of NIST's related publications.

⁵⁶Internet of Things Cybersecurity Improvement Act of 2020, Pub. L. No: 116-207, 134 Stat. 1001, 1002 (Dec. 4, 2020), 15 U.S.C. § 278g-3b.

⁵⁷National Institute of Standards and Technology, *IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements*, Special Publication 800-213 (Gaithersburg, MD: November 2021), and *IoT Device Cybersecurity Guidance for the Federal Government: IoT Device Cybersecurity Requirement Catalog*, Special Publication 800-213A (Gaithersburg, MD: November 2021).

⁵⁸Established in 2016, NIST's Cybersecurity for IoT Program aims to (1) support the development and application of standards, guidelines, and related tools to improve the cybersecurity of connected devices and the environments in which they are deployed; (2) collaborate with stakeholders across government, industry, international bodies, and academia; and (3) cultivate trust and foster an environment that enables innovation on a global scale.

⁵⁹See National Institute of Standards and Technology, *Foundational Cybersecurity Activities for IoT Device Manufacturers*, NIST Interagency Report (NIST IR) 8259 (May 2020) and *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks*, NIST IR 8228 (June 2019).

Table 7: National Institute of Standards and Technology (NIST) Key Publications on Internet of Things (IoT) Cybersecurity

Publication	Description
NIST Interagency Report (NIST IR) 8228, <i>Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks</i> (June 2019)	Intended to help federal agencies and other organizations ^a better understand and manage the cybersecurity and privacy risks associated with their individual IoT devices throughout the devices' life cycles. Identifies considerations that may affect the management of cybersecurity and privacy risks for IoT devices as compared to conventional IT devices and describes ways that organizations can mitigate IoT cybersecurity and privacy risks.
NIST IR 8259, <i>Foundational Cybersecurity Activities for IoT Device Manufacturers</i> (May 2020)	Intended to help manufacturers lessen the cybersecurity-related efforts needed by customers, which in turn can reduce the prevalence and severity of IoT device compromises and the attacks performed using compromised IoT devices. Describes recommended activities related to cybersecurity that manufacturers should consider performing before their IoT devices are sold to customers.
NIST IR 8259A, <i>IoT Device Cybersecurity Capability Core Baseline</i> (May 2020)	Intended to be used in conjunction with NIST IR 8259 and provides organizations a starting point for identifying the device cybersecurity capabilities for new IoT devices that they will manufacture, integrate, or acquire. Defines an <i>IoT Device Cybersecurity Capability Core Baseline</i> , which is a set of device capabilities generally needed to support common cybersecurity controls that protect an organization's devices as well as device data, systems, and ecosystems.
NIST IR 8259B, <i>IoT Non-Technical Supporting Capability Core Baseline</i> (August 2021)	Intended to be used in conjunction with NIST IR 8259 and NIST IR 8259A and provides organizations a starting point to use in identifying the non-technical supporting capabilities needed in relation to IoT devices they will manufacture, integrate, or acquire. Defines an IoT device manufacturers' non-technical supporting capability core baseline, which is a set of non-technical supporting capabilities generally needed from manufacturers or other third parties to support common cybersecurity controls that protect an organization's devices as well as device data, systems, and ecosystems.
Special Publication (SP) 800-213, <i>IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements</i> (November 2021)	Intended to help organizations consider how an IoT device they plan to acquire can integrate into a system. Provides information on considering system security from the device perspective, which allows for the identification of device cybersecurity requirements—the abilities and actions an organization will expect from an IoT device and its manufacturer or third parties, respectively.
SP 800-213A, <i>IoT Device Cybersecurity Guidance for the Federal Government: IoT Device Cybersecurity Requirement Catalog</i> (November 2021)	Provides a catalog of IoT device cybersecurity capabilities and non-technical supporting capabilities that can help organizations as they use SP 800-213 to determine and establish device cybersecurity requirements.
NIST IR 8425, <i>Profile of the IoT Core Baseline for Consumer IoT Products</i> (September 2022)	Builds on NIST IR 8259 series of documents for IoT device manufacturers and extends the IoT core cybersecurity baseline for consumer IoT products.

Source: GAO summary of NIST publications. | GAO-23-105327

^aIn NIST guidance, organization is meant to describe entities of any size, complexity, or positioning within an organizational structure (e.g., a federal agency or, as appropriate, any of its operational elements).

In addition to publications on IoT, NIST has also issued publications on the security of OT, including ICS (a specific subset of OT). For example, NIST's *Guide to Industrial Control Systems (ICS) Security*, issued in May

2015, describes steps that organizations can take to secure ICS.⁶⁰ In April 2022, NIST issued a draft update to this publication, NIST's *Guide to Operational Technology (OT) Security*, which expands the scope of the publication from ICS to OT and includes updated information on OT threats and vulnerabilities, risk management, recommended practices, and architectures, among other things.⁶¹ See table 8 for more information on NIST's cybersecurity publications.

Table 8: National Institute of Standards and Technology (NIST) Publications on Operational Technology (OT) Cybersecurity

Publication	Description
Special Publication (SP) 800-82 Revision 2, <i>Guide to Industrial Control Systems (ICS) Security</i> (May 2015)	Provides information intended to help organizations secure ICS, while addressing their unique performance, reliability, and safety requirements. Describes ICS and typical system topologies; identifies typical threats and vulnerabilities to these systems; and provides recommended security countermeasures to mitigate the associated risks.
SP 800-82 Revision 3 (Draft), <i>Guide to Operational Technology (OT) Security</i> (April 2022)	Expands the scope of SP 800-82 to include OT, not just ICS. Describes the application of the NIST Risk Management Framework and Cybersecurity Framework to OT, and provides an overlay of the NIST SP 800-53 Revision 5 ^a control catalog to further help organizations apply the NIST controls to OT.

Source: GAO summary of NIST publications. | GAO-23-105327

^aNational Institute of Standards and Technology, Special Publication 800-53, revision 5, Security and Privacy Controls for Information Systems and Organizations (Gaithersburg, MD: December 2020). This publication provides a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats and risks. The controls are flexible and customizable and implemented as part of an organization-wide process to manage risk.

National Cybersecurity Center of Excellence (NCCoE)

NIST's NCCoE has several projects related to the cybersecurity of IoT and OT technologies. See appendix II for a list of key NCCoE publications on the topic of IoT and OT cybersecurity.

For example:

- **Network Behavior of IoT Devices.** The NCCoE issued Draft NIST IR 8349, *Methodology for Characterizing Network Behavior of Internet of*

⁶⁰National Institute of Standards and Technology, *Guide to Industrial Control Systems (ICS) Security*, NIST Special Publication 800-82 Revision 2, (May 2015)

⁶¹National Institute of Standards and Technology, *Guide to Operational Technology (OT) Security*, NIST Special Publication 800-82 Revision 3 (Draft), (April 2022).

Things Devices, in January 2022.⁶² This draft publication demonstrates how to use an open source tool to describe the communication requirements of IoT devices. According to the draft publication, manufacturers and network administrators can use the techniques and tools described in the publication for capturing network communications from IoT devices and analyzing network captures to help ensure IoT devices perform as intended.

- **Trusted IoT Device Network-Layer Onboarding project.** Launched in May 2021, this project is intended to focus on secure approaches to managing IoT devices' ability to access an organization's network. According to the NCCoE website, the center will build a trusted network-layer onboarding solution example using commercially available technology that will address a set of cybersecurity challenges aligned to the NIST Cybersecurity Framework.⁶³ The project is planned to result in a freely available NIST cybersecurity practice guide by the end of fiscal year 2023.

IoT Working Group and Advisory Board

In response to requirements in the FY2021 NDAA,⁶⁴ in December 2021, NIST, acting on behalf of the Department of Commerce, formed a working group comprised of stakeholders from 15 departments and agencies across the federal government. According to the act, the working group is to, among other things,

- identify any federal regulations, statutes, grant practices, budgetary or jurisdictional challenges, and other sector-specific policies that are inhibiting, or could inhibit, the development or deployment of the IoT; and
- examine (1) how agencies can benefit from utilizing IoT; (2) the use of IoT by agencies; (3) the preparedness and ability of agencies to adopt IoT technology; and (4) any additional security measures that agencies may need to take to safely and securely use IoT, including measures that ensure the security of critical infrastructure and

⁶²National Institute of Standards and Technology's National Cybersecurity Center of Excellence, *Methodology for Characterizing Network Behavior of Internet of Things Devices*, (January 2022).

⁶³National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity* (Gaithersburg, MD: Feb. 12, 2014). Version 1.1 of the framework was issued Apr. 16, 2018.

⁶⁴William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283 § 9204, 134 Stat. 4797 (Jan. 1, 2021), 47 U.S.C. § 901 note.

enhance the resiliency of federal systems against cyber threats to the IoT.

Subsequently, in January 2022, NIST established a steering committee and in October 2022, NIST appointed 16 stakeholders from outside the federal government with expertise in IoT to the committee. The act states that the steering committee is to provide recommendations to the working group by January 2022 and the working group is to provide a report to Congress on aspects of IoT by July 2022. According to NIST officials, the committee is expected to present its findings approximately one year after its final formation, and the working group is to report to Congress in spring 2024.

Cybersecurity Labels for Consumer IoT Devices

In May 2021, the President issued Executive Order 14028 on improving cybersecurity and directed NIST to initiate pilot product labeling programs for consumer IoT products and consumer software products.⁶⁵ The programs are to educate the public on the security capabilities of IoT devices and software development practices, and to consider ways to encourage manufacturers and developers to participate in them. The order also required NIST to submit a report to the Assistant to the President for National Security Affairs within one year describing the programs' effectiveness and possible improvements.

On May 10, 2022, NIST delivered a summary report about the cybersecurity labeling programs to the Assistant to the President for National Security Affairs.⁶⁶ Reflecting consultations with the private sector and relevant agencies, the report describes the pilot programs as well as opportunities for improvements.

⁶⁵Executive Order 14028, *Improving the Nation's Cybersecurity* (May 12, 2021).

⁶⁶National Institute of Standards and Technology, *Report for the Assistant to the President for National Security Affairs (APNSA) on Cybersecurity Labeling for Consumers: Internet of Things (IoT) Devices and Software* (Gaithersburg, MD: May 2022).

Federal Acquisition Regulatory Council is Considering Guidance Updates to Better Manage IoT and OT Cybersecurity Risks

As stated earlier, the Federal Acquisition Regulatory Council is responsible for managing changes in the FAR.⁶⁷ Revisions to the FAR are prepared and issued through the coordinated action of two councils, the Defense Acquisition Regulations Council and the Civilian Agency Acquisition Council.

According to Federal Acquisition Regulatory Council officials, as of September 2022, the Council was considering whether NIST guidance on IoT cybersecurity⁶⁸ as well as related requirements for OT in Executive Order 14028⁶⁹ may require changes to the FAR. The officials told us that the Council was considering several potential changes to the FAR that affect cybersecurity, including cybersecurity risks associated with IoT and OT devices. Table 9 contains examples of potential changes to the FAR that may affect cybersecurity associated with IoT and OT devices.

Table 9: Examples of Potential Changes to the Federal Acquisition Regulation (FAR) Affecting IoT and OT Cybersecurity (September 2022)

Proposed FAR changes (by Federal Acquisition Regulatory Council-identified case number)	Description
FAR case 2017-016, "Controlled Unclassified Information"	Would implement regulations to address agency policies for designating, safeguarding, disseminating, marking, and disposing of controlled unclassified information, including such information stored on or processed by Internet of Things (IoT) and operational technology (OT). As of September 2022, Office of Management and Budget's (OMB) Office of Federal Procurement Policy has identified draft rule issues and OMB and FAR and Defense Acquisition Regulations Council (DARC) ^a staff are resolving issues.

⁶⁷The Federal Acquisition Regulatory Council was established to assist in the direction and coordination of Government-wide procurement policy and Government-wide procurement regulatory activities in the Federal Government, in accordance with Title 41, Chapter 7, Section 421 of the Office of Federal Procurement Policy (OFPP) Act. The Administrator, in consultation with the Council, shall ensure that procurement regulations, promulgated by executive agencies, are consistent with the Federal Acquisition Regulation (FAR) and in accordance with any policies issued pursuant to Section 405 of Title 41. The Council manages coordinates, controls, and monitors the maintenance and issuance of changes in the FAR.

⁶⁸National Institute of Standards and Technology, *IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements*, Special Publication 800-213 (Gaithersburg, MD: November 2021).

⁶⁹The White House, *Improving the Nation's Cybersecurity*, Executive Order 14028 (Washington, D.C.: May 12, 2021).

Proposed FAR changes (by Federal Acquisition Regulatory Council-identified case number)	Description
FAR cases 2018-017, "Prohibition on Certain Telecommunications and Video Surveillance Services or Equipment," and 2019-009, "Prohibition on Contracting with Entities Using Certain Telecommunications and Video Surveillance Services or Equipment"	Would prohibit the procurement of certain telecommunications and video surveillance equipment and services, including IoT and OT, from several foreign technology companies. As of September 2022, the Department of Defense, General Services Administration, and National Aeronautics and Space Administration are processing the FAR rule.
FAR case 2020-011, "Implementation of Federal Acquisition Security Council Exclusion Orders"	Would implement a process in which the recommendations of the Federal Acquisition Security Council to exclude certain products, services, or sources, to include IoT and OT, from the federal supply chain are implemented. As of September 2022, DARC and FAR staff are resolving open issues with the rule.
FAR case 2021-017, "Cyber Threat and Incident Reporting and Information Sharing"	Would implement requirements of Executive Order 14028 relating to sharing of information about cyber threats and incident information and reporting cyber incidents, to include information related to IoT and OT devices. As of September 2022, DARC and FAR staff are resolving open issues with the rule.
FAR case 2021-019, "Standardizing Cybersecurity Requirements for Unclassified Federal Information Systems"	Would implement requirements of Executive Order 14028 relating to standardizing common cybersecurity contractual requirements across federal agencies for unclassified federal information systems, including IoT or OT located within the boundary of the system, pursuant to the Department of Homeland Security recommendations. As of September 2022, DARC and FAR staff are resolving open issues with the rule.
FAR case 2019-018, "Federal Acquisition Supply Chain Security Act of 2018"	Would partially implement a section of the Federal Acquisition Supply Chain Security Act of 2018. This law, part of the SECURE Technology Act, establishes the Federal Acquisition Security Council and its functions and authorities as well as supply chain risk assessment requirements for executive agencies.
FAR case 2019-014, "Strengthening America's Cybersecurity Workforce"	Would implement Executive Order 13870, America's Cybersecurity Workforce, which directs agencies to incorporate the National Initiative for Cybersecurity Education Framework lexicon and taxonomy into contracts for IT and cybersecurity services. Contracts for IT and cybersecurity services must include reporting requirements that will enable agencies to evaluate whether personnel have the necessary knowledge and skills to perform the tasks specified in the contract, consistent with the framework. As of September 2022, DARC and FAR staff are resolving open issues with the rule.

Source: GAO analysis of Federal Acquisition Regulatory Council data. | GAO-23-105327

^aThe Defense Acquisition Regulations Council and the Civilian Agency Acquisition Council, and their respective staff work together to develop and update the FAR.

Selected SRMAs Did Not Measure Effectiveness of IoT and OT Efforts or Assess Cybersecurity Risks

While the three selected sectors' SRMAs reported various IoT and OT cybersecurity efforts, none of the SRMAs have evaluated the effectiveness of these. Further, the SRMAs have not conducted cybersecurity risk assessments specific to their sectors' IoT and OT environments. Industry representatives from selected sectors' SCCs and ISACs reported challenges in managing cybersecurity vulnerabilities through SRMAs and CISA. Key entities acknowledged these challenges and recommended improvements to cyber threat sharing.

SRMAs Reported Various Efforts to Enhance the Cybersecurity of the Sectors' IoT and OT Environments

Although the private sector owns the majority of the nation's critical infrastructure, CISA, the SRMAs, and the private sector work together to protect these assets and systems. Presidential Policy Directive 21, issued in February 2013, assigned to DHS the responsibility for coordinating the overall federal effort to promote the security and resilience of the nation's critical infrastructure.⁷⁰ In addition, the FY2021 NDAA assigned the SRMAs responsibility for efforts, including providing specialized expertise that support their respective sectors, such as assessment and prioritizing of risks and consideration of cybersecurity threats, vulnerabilities, and risks.⁷¹ SRMAs described various efforts supporting the cybersecurity of their sectors' IoT and OT environments.

Department of Energy

Energy officials stated that the department's office of Cybersecurity, Energy Security, and Emergency Response (CESER) primarily fulfills the agency's SRMA role for the energy sector. While Energy does not have guidance specifically targeted to IoT, department officials stated that they support a portfolio of research and development projects specifically targeted to enhance the security and resilience of energy delivery systems. Department officials cited several examples of research projects intended to address IoT risks. These examples include:

- **The Pacific Northwest National Laboratory's Universal Utility Data Exchange.** This research project is intended to improve secure communications with IoT devices by developing a more secure and flexible communication protocol for IoT data exchanges.
- **The University of Arkansas Automated Vulnerability Intelligence and Risk Assessment project.** This research project is intended to mitigate the increased risks of expanding IoT applications by automatically collecting asset and configuration data, identifying assets affected by vulnerabilities, and visually presenting risk data to security operators.

In addition, Energy officials reported that OT comprises the majority of the technology used for sector operations. The department had developed

⁷⁰The White House, *Presidential Policy Directive 21: Critical Infrastructure Security and Resilience* (Washington, D.C.: Feb. 12, 2013).

⁷¹William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283 § 9002, 134 Stat. 3388, 4770 - 4771 (Jan. 1, 2021), adding § 2215 to the Homeland Security Act of 2002, 6 U.S.C. § 665d(c).

guidance and resources specifically for the OT environment. Examples of these guidance documents and resources include:

- **The Cybersecurity Capability Maturity Model version 2.1 June 2022.**⁷² This free tool is intended to help organizations evaluate their cybersecurity capabilities and optimize security investments. The guidance provided in this publication is intended to address the implementation and management of cybersecurity practices associated with IT and OT assets and the environments in which they operate.
- **Considerations for ICS/OT Cybersecurity Monitoring Technologies.** This guidance provides suggested evaluation considerations for technologies to monitor ICS and OT cybersecurity for visibility on entities systems. This was developed and published in connection with the 100-day plan described below.⁷³
- **100-Day Action Plan for the U.S. Electricity Subsector.** This initiative was launched in April 2021 and led by CESER in close coordination with CISA and electric industry stakeholders. The plan leveraged the important public-private partnerships to improve the security of the OT and ICS that manage the nation’s electric systems, by enhancing the visibility, detection, and monitoring of these critical networks.⁷⁴
- **Cyber Testing for Resilient ICS.** This program, also known as CyTRICS, partners across stakeholders to identify high priority OT components, perform expert testing, share information about vulnerabilities in the digital supply chain, and inform improvements in component design and manufacturing.
- **Cybersecurity for the Operational Technology Environment.** This methodology, also known as CyOTE, aims to enhance energy sector threat detection of anomalous behavior potentially indicating malicious cyber activity in OT networks.

⁷²Department of Energy, *The Cybersecurity Capability Maturity Model version 2.1* (June 2022).

⁷³Department of Energy, “*Considerations for ICS/OT Cybersecurity Monitoring Technologies*,” accessed March 2022, <https://www.energy.gov/ceser/considerations-icsot-cybersecurity-monitoring-technologies>.

⁷⁴Department of Energy, *DOE Kicks Off 100-Day Plan to Address Cybersecurity Risks to the U.S. Electric System, Seeks Input from Stakeholders on Safeguarding U.S. Critical Energy Infrastructure* (Washington, D.C.: Apr. 20, 2021).

Department of Health and
Human Services

- **Cybersecurity Risk Information Sharing Program.** This program, also known as CRISP, is a public-private partnership that delivers relevant and actionable cybersecurity information to participants from the U.S. electricity industry. The purpose of the program is to collaborate with energy sector partners to facilitate the timely bi-directional sharing of unclassified and classified threat information.

Department of Health and Human Services (HHS) officials stated that the Office of the Assistant Secretary for Preparedness and Response, Critical Infrastructure Protection Division fulfills HHS's role as the SRMA for the healthcare and public health sector. Program support for the sector is carried out via various task groups that convene to work on guidance and threat information for the sector.

Additionally, the Assistant Secretary for Preparedness and Response works closely with CISA, the Federal Bureau of Investigation, and the Food and Drug Administration (FDA) to disseminate threat information related to IoT medical devices.⁷⁵ This information is communicated in a weekly newsletter, which contains cyber threat information from the Health Sector Cybersecurity Coordination Center,⁷⁶ CISA, and the Federal Bureau of Investigation, and ad-hoc cyber bulletins and targeted briefings in response to specific threats.

Additionally, the Center for Devices and Radiological Health within the FDA has developed guidance on the cybersecurity of IoT medical devices under FDA regulatory oversight. The guidance documents include those described below.

- **Medical Device Safety Action Plan.**⁷⁷ The plan outlines how the FDA will encourage innovation to improve safety, detect safety risks earlier, and keep doctors and patients better informed.

⁷⁵As noted earlier, HHS officials stated that IoT includes network-connected medical devices.

⁷⁶The Health Sector Cybersecurity Coordination Center was established to improve cybersecurity information sharing among HHS, its federal partners, and the sector.

⁷⁷Food and Drug Administration, *Medical Device Safety Action Plan: Protecting Patients, Promoting Public Health* (2018).

- **Playbook for Threat Modeling Medical Devices.**⁷⁸ The document, commissioned by the FDA and co-authored by MITRE Corporation and the Medical Device Innovation Consortium, is intended to increase the knowledge of threat modeling throughout the medical device ecosystem in order to further strengthen the cybersecurity and safety of medical devices.
- **Premarket Guidance for Management of Cybersecurity.**⁷⁹ The guidance identifies issues related to cybersecurity that manufacturers should consider in the design and development of their medical devices as well as in preparing premarket submissions for those devices.
- **Post-market Management of Cybersecurity in Medical Devices.**⁸⁰ This guidance is intended to inform industry and FDA staff of the agency's recommendations for managing postmarket cybersecurity vulnerabilities for marketed and distributed medical devices.

As co-SRMAs, DHS and DOT lead the transportation systems sector. According to DHS, the Transportation Security Administration (TSA) and the U.S. Coast Guard fulfils DHS's role as executive agents for the sector.⁸¹ TSA officials noted that they have focused more on OT security due to the threat landscape, to include threat briefings specific to OT. For example, TSA has issued threat briefings specific to OT and published a Surface Transportation Cybersecurity toolkit designed to provide informative cyber risk management tools and resources.⁸² Additionally, TSA issued security directives, for higher risk railroads and rail transit and pipeline owner/operators that require certain actions to improve cybersecurity preparedness. The actions include appointment of cybersecurity coordinators, reporting of cybersecurity incidents to CISA, conducting a cybersecurity vulnerability assessment, and development of

⁷⁸The MITRE Corporation and the Medical Device Innovation Consortium, *Playbook for Threat Modeling Medical Devices* (November 2021).

⁷⁹Food and Drug Administration, *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices*, (October 2014), draft update dated April 2022.

⁸⁰Food and Drug Administration, *Post-market Management of Cybersecurity in Medical Devices, Guidance for Industry and Food and Drug Administration Staff* (Silver Spring, MD: December 2016).

⁸¹Both TSA and the U.S. Coast Guard are component agencies of DHS.

⁸²Transportation Security Administration, "Surface Transportation Cybersecurity Resource Toolkit" accessed July 11, 2022, <https://www.tsa.gov/for-industry/surface-transportation-cybersecurity-toolkit>.

cybersecurity incident response plans.⁸³ TSA also distributed an information circular recommending the same actions for lower risk railroads, public transportation, and over-the-road buses.⁸⁴ Separately, the U.S. Coast Guard has issued cybersecurity guidance for regulated facilities.⁸⁵ However, the guidance does not address IoT or OT cybersecurity.

DOT officials stated that the Office of the Secretary/Office of Intelligence, Security, and Emergency Response/National Security Policy and Preparedness Division fulfills Transportation's role as co-SRMA for the sector. Department officials stated that they have established various mechanisms for collaboration in research and development as well as general IT and OT support that help facilitate enhancement of cybersecurity for the sector. For example, DOT conducts an IoT cybersecurity research program through its Intelligent Transportation Systems Joint Program Office.

These resources, which include security directives and information circulars, however, are primarily for IT and OT and are not specific to IoT. Support efforts by Transportation does not include guidance specifically for IoT. Additionally, DHS and DOT do not currently have any plans to provide specific IoT guidance for the sector.

Selected SRMAs Have Not Measured the Effectiveness of Their IoT and OT Efforts

According to the 2013 National Plan, SRMAs should use metrics and other evaluation procedures to measure the progress and assess the effectiveness of their efforts that support their sectors and enhance the

⁸³Department of Homeland Security, Transportation Security Administration, *Enhancing Rail Cybersecurity*, Security Directive 1580-21-01 (Springfield, Virginia: Dec. 31, 2021); *Enhancing Public Transportation and Passenger Railroad Cybersecurity*, Security Directive 1582-21-01, (Springfield, Virginia: Dec. 31, 2021); *Revision to the Security Directive Pipeline-2021-02 series: Pipeline Cybersecurity Mitigation Actions, Contingency Planning, and Testing*, Security Directive Pipeline-2021-02C (Springfield, Virginia: July 27, 2022); and *Enhancing Pipeline Cybersecurity*, Security Directive Pipeline-2021-01B (Springfield, Virginia: May 29, 2022).

⁸⁴Department of Homeland Security and Transportation Security Administration, *Surface Transportation IC-2021-01, Enhancing Surface Transportation Cybersecurity* (Springfield, Virginia: Dec. 31, 2021).

⁸⁵U.S. Coast Guard, *Navigation and Vessel Inspection Circular Number 01-20, Guidelines for Addressing Cyber Risks at Maritime Transportation Security (MTSA) Act Regulated Facilities* (Washington, D.C.: Feb. 26, 2020).

cybersecurity of critical infrastructure.⁸⁶ In addition, DHS's Critical Infrastructure Risk Management Framework states that use of metrics and other evaluation procedures to measure progress and assess the effectiveness of efforts to secure and strengthen the resilience of critical infrastructure informs the process of prioritizing and selecting the most effective and cost-efficient ways to manage risk.⁸⁷ According to the Framework, assessing effectiveness could include developing metrics to indicate the effectiveness of security and resilience activities and the extent to which these activities are reducing risks.

However, as of September 2022, none of the SRMAs for the selected sectors in this review had developed qualitative or quantitative metrics to measure the effectiveness of their efforts to enhance the cybersecurity of their sectors' IoT and OT environments. SRMA officials have stated that it can be difficult to identify an overall assessment of program effectiveness, particularly when an SRMA is relying on sector entities to voluntarily provide relevant information.

According to DHS's 2013 National Plan, each critical infrastructure sector should update its sector-specific plan every 4 years to, among other things, develop metrics to measure progress on achieving sector goals. However, the current plans date from 2015 and 2016.⁸⁸ In order to reflect changes in law and policy regarding SRMAs, CISA officials noted that they are leading an effort to update the National Plan, expected by the first quarter of 2023.

According to CISA officials, the updated National Plan will encourage each sector to develop sector-specific plans that may include additional sector-specific effectiveness and programmatic measures. CISA officials estimated that these updated sector-specific plans will follow the updated National Plan but they did not provide a timeframe.

⁸⁶Department of Homeland Security, *National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience* (2013).

⁸⁷Department of Homeland Security, *Supplemental Tool: Executing A Critical Infrastructure Risk Management Approach*.

⁸⁸We have previously recognized the need for updated sector-specific plans in multiple sectors. See GAO, *Critical Infrastructure Protection: CISA Should Assess the Effectiveness of its Actions to Support the Communications Sector*, [GAO-22-104462](#), (Washington, D.C.: Nov. 23, 2021) and *Critical Infrastructure Protection: Treasury Needs to Improve Tracking of Financial Sector Cybersecurity Risk Mitigation Efforts*, [GAO-20-631](#) (Washington, D.C. Sep. 17, 2020).

Until the SMRAs establish IoT and OT specific metrics, they will be unable to fully measure the effectiveness of their efforts to improve the cybersecurity of critical infrastructure. Establishing metrics, as part of sector-specific plans, will provide a basis for SRMAs to establish accountability, document actual performance, promote effective management, and provide a feedback mechanism to inform decision making.

SRMAs Have Not Conducted Cybersecurity Risk Assessments That Focused on IoT and OT

The NDAA for FY 2021 requires SRMAs to assess sector risks including identifying and prioritizing risks within the designated sector or subsector.⁸⁹ Further, according to NIST, as part of the risk management process, organizations should assess the level of risk introduced by IoT devices. These devices may require additional security controls or the introduction of compensating controls to reduce risk.⁹⁰

However, the SRMAs (Energy, HHS, and DHS in coordination with DOT) have not conducted sector-wide cybersecurity risk assessments specific to IoT and OT devices. Although industry officials reported cybersecurity risks that may include IoT and OT, the risks were similar throughout the sectors and were often grouped with general threats and vulnerabilities to traditional IT, such as ransomware⁹¹ and phishing.⁹²

Specifically, as part of their broader risk management efforts, two SRMAs (Energy, and DHS in coordination with DOT) noted that they focus on potential threats to OT and one SRMA (HHS) touched on risks to a specific type of IoT (medical devices). However, none of these efforts suffice as a comprehensive sector-wide cybersecurity risk assessment specific to IoT and OT devices. Below are descriptions of how each of the SRMAs addresses IoT and OT in their broader risk assessments.

⁸⁹William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283 § 9002, 134 Stat.3388, 4770 - 4771 (Jan. 1, 2021) adding sec. 2215 to the Homeland Security Act of 2002, 6 U.S.C. § 665d(c).

⁹⁰National Institute of Standards and Technology, *IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements*, Special Publication 800-213 (November 2021).

⁹¹Ransomware is a form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. <https://www.cisa.gov/stopransomware>.

⁹²Phishing is a form of social engineering. Phishing attacks use email or malicious websites to solicit personal information by posing as a trustworthy organization. <https://www.cisa.gov/uscert/ncas/tips/ST04-014>.

-
- **Department of Energy.** Energy officials stated they assessed cybersecurity risks for the sector using a variety of information sharing tools. These tools are mechanisms that organizations within the sector can use to assess their own network environment risks. However, these tools and resources look at risks as a whole across the sector and are not specific to any one technology, such as IoT or OT. While the department has ongoing risk activities for OT, it has yet to conduct a sector-wide assessment specific to IoT and OT.

Additionally, the department's Energy Efficiency and Renewable Energy office's May 2021 Cybersecurity Multiyear Program Plan acknowledged that the increasing interconnectivity of technologies and devices increases the overall cyber vulnerability and need to improve the cyber resilience, including IoT devices.⁹³ The plan noted that cyber threats continue to target critical OT, including energy delivery systems and ICSs as reported by DHS's US-CERT.

- **Department of Health and Human Services.** HHS officials reported that their risk management activities are primarily focused on IoT medical devices' impact to the sector. In addition, officials stated that the department performs high-level threat assessments for the sector based on information obtained from CISA, the Federal Bureau of Investigation, and intelligence agencies. Further, FDA officials stated that the agency leads the medical device risk assessments for IoT and OT, and has extensive engagement across the sector in managing medical device risks. However, while HHS has ongoing risk activities for IoT medical devices, it has yet to conduct a sector-wide risk assessment specific to IoT and OT.
- **Departments of Homeland Security and Transportation.** Transportation officials reported that the 2015 Transportation Systems Sector-Specific Plan identified sector risks that remain valid today. However, DOT officials stated they, in coordination with DHS, have not collected information explicitly related to IoT and OT devices used across the sector from the private sector owners and operators that control the vast majority of sector critical infrastructure. Further, officials stated the department is not fully aware of how OT is being used in the sector. Officials explained that there have not been any specific efforts to determine IoT and OT usage sector-wide, because cybersecurity is not narrowly focused on one technology.

⁹³Department of Energy, *EERE Cybersecurity Multiyear Program Plan: Report to Congress, Revised May 2021* (Washington, D.C.: May 2021).

According to the SRMAs and CISA officials, IoT and OT devices are generally considered to be a component of IT overall, and hence are not tracked separately. However, according to NIST guidance, part of understanding IoT device cybersecurity requirements involves first understanding IoT device uses and benefits, and then understanding the device's impact to system risk assessments. NIST guidance notes that organizations should remember that the incorporation of an IoT device could alter the information system's risk assessment. It further adds that once aware of existing IoT usage, organizations need to understand how the characteristics of IoT devices affect managing risk response. According to NIST guidance, it is important that organizations understand their use of IoT because many of these devices affect cybersecurity and privacy risks differently than conventional IT devices.⁹⁴

The need for understanding the IoT and OT environments is further amplified by cyber incidents affecting IoT and OT, such as CISA's alert for a heightened distributed denial-of-service threat posed by botnets. In a July 2020 report issued by the Department of Commerce and DHS, it noted that botnets will continue to grow in sophistication and will expand to even more types of IoT products.

Further, an industry review of 2021 incidents stated that ransomware mainly targets enterprise IT systems; however, there are a number of instances when it has impacted OT directly as well as integrated IT and OT environments.⁹⁵ The review assessed with high confidence that ransomware will continue to disrupt industrial operations and OT environments. Given these type of attacks and their potential impact, it is important for sectors to explicitly include IoT and OT devices as part of their required risk assessments because of the expanded threat landscape and interconnectedness that these technologies introduce.

Additionally, in its 2022 draft IT and OT convergence report, the President's National Security Telecommunications Advisory Committee recommended that civilian executive departments and agencies maintain a real-time, continuous inventory of all OT devices, software, systems, and assets within their area of responsibility, including an understanding

⁹⁴National Institute of Standards and Technology, *IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements*, Special Publication 800-213 (November 2021) and *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks*, NISTIR 8228 (June 2019).

⁹⁵Dragos, *ICS/OT Cybersecurity Year in Review, 2021* (Washington, D.C.: 2022).

of any interconnectivity to other systems.⁹⁶ It noted that once federal agencies clearly understand the vast and interconnected nature of their OT devices and infrastructure, they can then make risk-informed decisions. Without conducting sector-wide risk assessments, to include IoT and OT devices, organizations will not know what additional security protections could be needed to address growing and evolving threats.

Industry Representatives Reported Challenges in Working with CISA; Key Entities Recommended Improving Threat Information Sharing

Challenges Reported by Industry Representatives

Industry representatives from each of the selected critical infrastructure sectors reported that they regularly meet with their respective SRMAs through set meetings and working groups. However, each have reported challenges with CISA in managing cybersecurity vulnerabilities associated with their sector. Specifically, industry representatives reported that the distributed threat and vulnerability information and guidance are not always timely, actionable, or specific to the needs of their respective sector or subsector. Further, some industry representatives reported the lack of coordination between CISA and their SRMAs as a challenge. In addition, industry representatives from a subsector noted that despite receiving threat information, they lacked the capacity to address the cybersecurity needs of and for the sector.

Lack of Timely, Actionable Guidance. Energy sector representatives noted that they often receive high-level or general information on threats and potential vulnerabilities that may not be useful to them or was received well after a threat was discovered. Energy sector representatives further expressed the desire to receive information that is actionable, timely, and more relevant to the needs of their sector and subsector for industry implementation.

In addition, aviation subsector officials also noted that while TSA and CISA provide the sector with information, there are issues with getting information in a timely and actionable manner, including the low

⁹⁶National Security Telecommunications Advisory Committee, *Draft NSTAC Report to the President: Information Technology and Operational Technology Convergence* (August 2022).

participation rate in high-level classified briefings due to members' lack of security clearance level or the limited time to schedule briefings.

Industry representatives from the mass transit and passenger rail subsector stated that they lacked information from TSA regarding threats and vulnerabilities specific to the subsector. Representatives expressed that the subsector needs more information on threats that are timely and targeted specifically to the subsector's OT environment before TSA issues a security directive. They noted that they would like coordination that is more robust because the response required incurs substantial costs to the subsector, which has limited resources.⁹⁷

Insufficient Coordination. Further, representatives from the healthcare and public health sector noted a lack of cohesiveness between HHS and CISA's direction on cybersecurity issues. They also noted that additional coordination would be more productive and less confusing for them. For example, representatives stated that at times the actions they should take were unclear when the information was distributed by CISA and not HHS or vice versa.

Lack of Resources and Support. Additionally, industry representatives from the maritime transportation systems subsector noted that coordination across the organization is critical due to the lack of cybersecurity professionals in the subsector. Representatives from the maritime transportation systems subsector expressed concern that there is a lack of operational support to assist with the implementation of recommended federal guidance, and further noted that guidance such as webinars, training, and exercise development would be beneficial.

Improvements Recommended
by Key Oversight Entities for
Addressing Cyber Threat
Information Sharing

Two key entities, DHS's Office of the Inspector General and the President's National Security Telecommunications Advisory Committee, acknowledged the information sharing challenges and recommended improvements in the area. Specifically, in August 2022, DHS's Office of the Inspector General found that CISA shared cyber threat information

⁹⁷According to a security directive from TSA designed to enhance public transportation and passenger railroad cybersecurity, certain large organizations in the sector are required to have a designated cybersecurity coordinator to be available to TSA and CISA 24 hours a day, seven days a week.

with participants in its Automated Indicator Sharing program.⁹⁸ However, it noted that the quality of information shared with participants was not always adequate to identify and mitigate cyber threats.⁹⁹ The report noted that most of the cyber threat indicators did not contain enough contextual information to help decision makers take action. The Inspector General recommended, among other things, that CISA develop and implement a formal process to verify the number of cyber threat indicators and defensive measures shared through CISA's Automated Indicator Sharing capabilities to enable accurate reporting and oversight. The report noted that CISA is currently taking actions to help address this issue.

Further, in its 2022 draft report on IT and OT convergence, the President's National Security Telecommunications Advisory Committee recommended that the National Security Council, CISA, and the Office of the National Cybersecurity Director should prioritize the development and implementation of interoperable, technology-neutral, vendor-agnostic information sharing mechanisms. This would enable the real-time sharing of sensitive information between authorized stakeholders involved with securing U.S. critical infrastructure. The report notes that the information sharing mechanisms should include breaking down the artificial barriers for sharing controlled unclassified information, both within the federal government and between the federal government and other key, cross-sector stakeholders.

We have ongoing work examining cyber threat information sharing with federal agencies, including challenges to effective sharing and the actions that federal agencies are taking to address them. We plan to report in winter 2023 on the results of our work.

⁹⁸DHS's Automated Indicator Sharing program is to enable the real-time exchange of unclassified cyber threat information and defensive measures to participants of the community. CISA offers the service at no cost to participants as part of CISA's mission to work with public and private sector partners to identify and help mitigate cyber threats through information sharing.

⁹⁹Department of Homeland Security, Office of the Inspector General, *Additional Progress Needed to Improve Information Sharing under the Cybersecurity Act of 2015*, OIG-22-59 (August 16, 2022).

NIST Has Issued Guidance, but OMB Has Not Established a Required Cybersecurity Waiver Process

The Internet of Things Cybersecurity Improvement Act of 2020 requires NIST to develop and publish standards and guidelines for the appropriate use and management by federal agencies of IoT devices.¹⁰⁰ The act also requires NIST to develop and publish guidelines for reporting, coordinating, publishing, and receiving information about security vulnerabilities relating to information systems, including IoT devices, in alignment with industry best practices and international standards.¹⁰¹

In response to the act, NIST issued IoT Device Cybersecurity Guidance in November 2021.¹⁰² This guidance is intended to be used by organizations in their acquisition processes as they acquire and integrate IoT devices into existing systems. In addition, in May 2022, NIST issued an update to its guidance *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*.¹⁰³ The publication describes the integration of supply chain risk management considerations into acquisition activities within every step of the procurement and contract management life cycle process. The publication also notes that this is essential to improving the management of cybersecurity risks throughout the supply chain. It further specifies that the practices and controls described for Cybersecurity Supply Chain Risk Management in the publication apply to both IT and OT environments and is inclusive of IoT.

To address the reporting of security vulnerabilities, NIST issued a draft special publication *Recommendations for Federal Vulnerability Disclosure*

¹⁰⁰Internet of Things Cybersecurity Improvement Act of 2020, Public Law No: 116-207 § 5, 134 Stat. 1004 (Dec. 4, 2020), 15 U.S.C. § 278g-3c.

¹⁰¹International Organization for Standardization/International Electrotechnical Commission (2018 and 2019): ISO/IEC 29147:2018 – Information technology – Security techniques – Vulnerability disclosure (ISO, Geneva, Switzerland). Available at <https://www.iso.org/standard/72311.html> and ISO/IEC 30111:2019 – Information technology – Security techniques – Vulnerability handling processes (ISO, Geneva, Switzerland). Available at <https://www.iso.org/standard/69725.html> (Sep. 20, 2022).

¹⁰²National Institute of Standards and Technology, *IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements*, Special Publication 800-213, (Gaithersburg, MD: November 2021).

¹⁰³National Institute of Standards and Technology, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations, Revision 1*, Special Publication 800-161, (May 2022).

Guidelines in June 2021.¹⁰⁴ According to NIST, the guidance establishes a flexible, unified framework for establishing policies and implementing procedures for reporting, assessing, and managing vulnerability disclosures for systems within the federal government, in alignment with international standards. Specifically, it recommends guidance for establishing a federal vulnerability disclosure framework and highlights the importance of properly handling vulnerability reports and ensuring clear communications to minimize or eliminate vulnerabilities. NIST notes that the framework also allows for local resolution support while providing federal oversight and should be applied to all software, hardware, and digital services under federal control. According to NIST, in 2020 alone, more than 18,000 vulnerabilities were publicly listed in the National Vulnerability Database.¹⁰⁵ NIST expects to finalize and publish the report by the second quarter of FY2023.

In addition to NIST's guidance on IoT cybersecurity, DHS, in coordination with the General Services Administration and the IT SCC, provided guidance in 2020 to the IT sector for security issues that agencies should consider when acquiring IoT technologies.¹⁰⁶ The guidance recommended improvements to the effectiveness of supply-chain, vendor, and technology evaluations prior to the purchase of IoT devices and services. These factors include, among other things, interconnection with legacy systems, that is, whether or not additional security controls need to be implemented in legacy systems when integrating IoT devices. These factors also include IoT Device Baseline Security, that is, whether the IoT meets the organization's minimum baseline security requirements for IoT. According to administration officials, the guidance is applicable to any critical infrastructure sector. In its 2022 draft report on IT and OT convergence, the President's National Security Telecommunications Advisory Committee recommended that CISA should work with the

¹⁰⁴National Institute of Standards and Technology, *Recommendations for Federal Vulnerability Disclosure Guidelines*, Special Publication 800-216 (Draft), (Gaithersburg, MD, June 7, 2021).

¹⁰⁵The National Vulnerability Database is the U.S. government repository of standards-based vulnerability management data that enables automation of vulnerability management, security measurement, and compliance. It includes databases of security checklist references, security-related software flaws, misconfigurations, product names, and impact metrics.

¹⁰⁶Department of Homeland Security and Cybersecurity and Infrastructure Security Agency, *Internet of Things: Security Acquisition Guidance for the Information Technology Sector* (2020).

General Services Administration to require the inclusion of risk-informed cybersecurity capabilities in procurement vehicles for the federal government.¹⁰⁷

OMB Has Yet to Establish a Required Cybersecurity Waiver Process for IoT

The Internet of Things Cybersecurity Improvement Act of 2020 requires that OMB develop and oversee the implementation of policies, principles, standards, or guidelines as may be necessary to address security vulnerabilities of information systems (including IoT devices). It also requires OMB to establish a standardized process for the Chief Information Officers (CIO) of covered federal agencies to follow when determining whether to waive the prohibition on procuring or using non-compliant IoT devices.¹⁰⁸

Under the act, agencies are prohibited from procuring or obtaining, renewing a contract to procure or obtain, or using an IoT device after December 4, 2022 if the CIO of a covered agency determines that the use of such device prevents compliance with the NIST-developed standards and guidelines.¹⁰⁹ The CIO of the agency may waive the prohibition if the CIO determines that at least one of the waiver criteria listed in the act has been met.¹¹⁰

To date, OMB has not yet developed guidance on security vulnerabilities. Consistent with the act, it is to do so if deemed necessary.

¹⁰⁷The President's National Security Telecommunications Advisory Committee (NSTAC), *Draft NSTAC Report to the President: Information Technology and Operational Technology Convergence*, (August 2022).

¹⁰⁸Internet of Things Cybersecurity Improvement Act of 2020, Pub. L. No. 116-207 § 7(b), 134 Stat. 1001, 1005 (Dec. 4, 2020), 15 U.S.C. § 278g-3e(b).

¹⁰⁹We refer to a "covered agency" because section 7 of the Internet of Things Cybersecurity Improvement Act of 2020 refers to a determination by an agency CIO under the contract review process established in 40 U.S.C. § 11319(b)(1)(C). This provision, added by the statute commonly known as the Federal Information Technology Acquisition Reform Act (FITARA), applies only to "covered agencies." Covered agencies are defined in 40 U.S.C. § 11319(a) as the 24 major departments and agencies listed in the Chief Financial Officers Act, 31 U.S.C. § 901 (FITARA has limited applicability to the Department of Defense). The Internet of Things Cybersecurity Improvement Act of 2020 otherwise uses a broader definition of "agency" from 44 U.S.C. § 3502. Pub. L. No. 116-207 § 3(1), 134 Stat. 1001 - 1002, 15 U.S.C. § 278g-3a(1).

¹¹⁰The waiver criteria established by the act are: (a) if the waiver is necessary in the interest of national security; (b) if procuring, obtaining, or using such device is necessary for research purposes; or (c) such a device is secured using alternative and effective means. Internet of Things Cybersecurity Improvement Act of 2020, Pub. L. No. 116-207 § 7(b), 134 Stat. 1005, 15 U.S.C. § 278g-3e(b).

Regarding the required standardized waiver process, as of November 22, 2022, OMB had not yet established such a process. OMB officials noted that the process required coordination and data gathering among OMB's Office of the Chief Information Officer and other entities to decide upon a standardized waiver process. OMB officials further noted that any waiver process would also need to include coordination with entities outside the federal civilian executive branch including with the intelligence community. According to OMB, it is targeting November 2022 for the release of guidance on the waiver process.

Given the act's restrictions on agency use of non-compliant IoT devices beginning in December 2022, it is vital for OMB to expeditiously establish a standardized waiver process for agencies. Without a standardized waiver process in place, agencies' use of IoT devices may not uniformly comply with established statutory waiver criteria or NIST-developed standards and guidelines for IoT devices security. As a result, any inconsistencies in agencies' non-standardized processes may increase the risk of inconsistencies in waiver decisions. We will continue to monitor OMB's efforts as part of our required biennial review of the waiver process, in accordance with the Internet of Things Cybersecurity Improvement Act of 2020.¹¹¹

Conclusions

Increasing cyber threats to critical infrastructure and their IoT and OT devices and systems represent a significant national security challenge. While guidance and resources have been developed to help manage cybersecurity risks to IoT and OT devices, selected SRMAs lack IoT and OT specific metrics to measure the effectiveness of their efforts. Until SRMAs establish IoT and OT specific metrics and update their sector specific plans to include those metrics, the effectiveness of their cybersecurity efforts will be unknown.

Further, none of the selected SRMAs have conducted sector-wide risk assessments specific to IoT and OT devices. Effective risk management of IoT and OT environments is essential to ensuring sector cybersecurity. Until SRMAs conduct sector-wide risk assessments that include IoT and OT, mitigation action priorities may not be focused on the risks with the most significant estimated adverse impact and frequency.

Additionally, OMB has not yet established a standardized IoT device cybersecurity waiver process for the CIOs of covered federal agencies, as

¹¹¹Subsequent reviews are due to Congress in December 2024 and 2026.

required by law. Absent a standardized cybersecurity waiver process, agencies will be at risk of inconsistently considering the use of non-compliant devices.

Recommendations for Executive Action

We are making a total of nine recommendations including two each to Energy, HHS, DHS, and DOT, and one to OMB. Specifically:

The Secretary of Energy, as SRMA for the energy sector, should direct the Director of the Office of Cybersecurity, Energy Security, and Emergency Response to use the National Plan to develop a sector-specific plan that includes metrics for measuring the effectiveness of their efforts to enhance the cybersecurity of their sector's IoT and OT environments. (Recommendation 1)

The Secretary of Energy, as SRMA for the energy sector, should direct the Director of the Office of Cybersecurity, Energy Security, and Emergency Response to include IoT and OT devices as part of the risk assessments of their sector's cyber environment. (Recommendation 2)

The Secretary of Health and Human Services, as SRMA for the healthcare and public health sector, should direct the Assistant Secretary for Preparedness and Response to use the National Plan to develop a sector-specific plan that includes metrics for measuring the effectiveness of their efforts to enhance the cybersecurity of their sector's IoT and OT environments. (Recommendation 3)

The Secretary of Health and Human Services, as SRMA for the healthcare and public health sector, should direct the Assistant Secretary for Preparedness and Response to include IoT and OT devices as part of the risk assessments of their sector's cyber environment. (Recommendation 4)

The Secretary of Homeland Security should direct the Administrator of the Transportation Security Administration and the Commandant of the U.S. Coast Guard to jointly work with the Department of Transportation's Office of Intelligence, Security and Emergency Response, as co-SRMAs for the transportation systems sector, to use the National Plan to develop a sector-specific plan that includes metrics for measuring the effectiveness of their efforts to enhance the cybersecurity of their sector's IoT and OT environments. (Recommendation 5)

The Secretary of Homeland Security should direct the Administrator of the Transportation Security Administration and the Commandant of the U.S.

Coast Guard to jointly work with the Department of Transportation's Office of Intelligence, Security and Emergency Response, as co-SRMAs for the transportation systems sector, to include IoT and OT devices as part of the risk assessments of their sector's cyber environment. (Recommendation 6)

The Secretary of Transportation should direct the Director, Office of Intelligence, Security and Emergency Response to jointly work with the Administrator of DHS's Transportation Security Administration and the Commandant of the U.S. Coast Guard, as co-SRMAs for the transportation systems sector, to use the National Plan to develop a sector-specific plan that includes metrics for measuring the effectiveness of their efforts to enhance the cybersecurity of their sector's IoT and OT environments. (Recommendation 7)

The Secretary of Transportation should direct the Director, Office of Intelligence, Security and Emergency Response to jointly work with the Administrator of DHS's Transportation Security Administration and the Commandant of the U.S. Coast Guard, as co-SRMAs for the transportation systems sector, to include IoT and OT devices as part of the risk assessments of their sector's cyber environment. (Recommendation 8)

The Director of OMB should, as required by the Internet of Things Cybersecurity Improvement Act of 2020,¹¹² expeditiously establish a standardized process for the Chief Information Officer of each covered agency to follow in determining whether the IoT cybersecurity waiver may be granted. (Recommendation 9)

Agency Comments and Our Evaluation

We provided a draft of this report for review and comment to Energy, HHS, DHS, DOT, and OMB, the agencies to which we made recommendations. We also provided a draft for comment to GSA, NASA, and NIST.

In an email, the Director of Office of Financial Policy and Audit Resolution at the Department of Energy told us the department did not plan to respond to our recommendations at this time. The Director added that the

¹¹²Internet of Things Cybersecurity Improvement Act of 2020, Pub. L. No. 116-207 § 7(b)(2), 134 Stat. 1005 (Dec. 4, 2020), 15 U.S.C. § 278g-3e(b).

Department would outline planned corrective actions after further interagency coordination with the other agencies mentioned in this report.

In its comments, reproduced in appendix III, HHS neither agreed nor disagreed with the recommendations but noted planned actions and challenges. Regarding our recommendation to develop a sector-specific plan that includes metrics, HHS noted that it planned to update its sector-specific plan upon release of the National Plan. It noted that the department cannot compel adoption of the plan in the private sector. It added, though, that the department would continue to work with other agencies in considering the development of metrics.

Because issuance of the updated National Plan is not expected until the first quarter of 2023, HHS could use the 2013 National Plan as an historical baseline to begin updating its sector-specific plan and considering metrics for IoT and OT cybersecurity efforts. We recognize the voluntary character of the relationship between HHS and the critical infrastructure sector. However, establishing IoT and OT specific metrics will provide a basis for HHS to establish accountability, document actual performance, promote effective management, and provide a feedback mechanism to inform decision-making.

Regarding our recommendation to include IoT and OT devices as part of the risk assessments of its sector's cyber environment, HHS noted that the organization responsible for SRMA activities does not have the capacity for an additional mission in IoT outside of medical devices. HHS also added that it takes a holistic approach to its cybersecurity responsibilities and will continue its risk assessment efforts. However, as stated earlier, organizations should assess the level of risk introduced by IoT devices because these devices may require additional security controls or the introduction of compensating controls to reduce risks. Without conducting sector wide risk assessments, including IoT and OT devices, agencies will not know what additional security protections may be needed to address growing and evolving threats.

In its comments, reproduced in appendix IV, DHS concurred with our recommendations and described actions to implement them. It stated that TSA, in coordination with the U.S. Coast Guard and DOT, is developing a draft sector-specific plan that is to include metrics for measuring effectiveness of efforts to enhance the cybersecurity of the sector's IoT and OT environments. It also stated that TSA had incorporated cybersecurity issues including OT and IoT in its sector risk assessment and noted that it would continue efforts to include IoT and OT devices in

risk assessments. DHS estimated that it will complete these efforts by June 28, 2024. DHS also provided technical comments that we incorporated as appropriate.

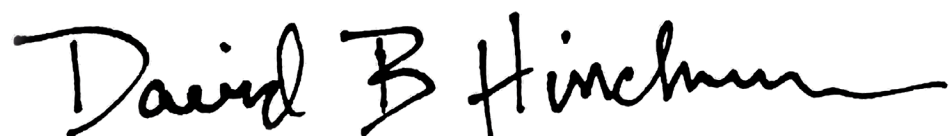
DOT's Audit Relations Analyst stated via email that DOT concurred with our recommendations. The Analyst also provided technical comments that we incorporated as appropriate.

In comments on our recommendation provided via email, OMB's Assistant General Counsel said that the agency is targeting November 2022 for release of guidance on the waiver process. However, as of November 22, 2022, OMB had not yet issued this guidance. The Assistant General Counsel also provided a technical comment that we incorporated as appropriate.

In an email, a Program Analyst from the Office of the Chief Financial Officer in the Office of Audit Management and Accountability indicated that GSA had no technical comments. The GAO/OIG Audit Liaison Program Manager from the Mission Support Directorate said in an email that NASA had no comments. In addition, the OIG/GAO Liaison from the Management and Organization Office of NIST provided technical comments via email that we incorporated as appropriate.

We are sending copies of this report to the appropriate congressional committees, the Secretaries of Commerce, Energy, Health and Human Services, Homeland Security, and Transportation, the Administrators of the General Services Administration and National Aeronautics and Space Administration, the Director of the Office of Management and Budget, 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 any questions about this report, please contact me at 214-777-5719 or at hinchmand@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 V.

A handwritten signature in black ink that reads "David B Hinchman". The signature is written in a cursive style with a long, sweeping underline.

David B. Hinchman
Acting Director, Information Technology and Cybersecurity

List of Committees

The Honorable Gary C. Peters
Chairman
The Honorable Rob Portman
Ranking Member
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Bennie G. Thompson
Chairman
The Honorable John Katko
Ranking Member
Committee on Homeland Security
House of Representatives

The Honorable Carolyn B. Maloney
Chairwoman
The Honorable James Comer
Ranking Member
Committee on Oversight and Reform
House of Representatives

Appendix I: Objectives, Scope, and Methodology

Our objectives were to (1) describe overall federal initiatives for managing cybersecurity risks associated with Internet of Things (IoT) and operational technology (OT) devices; (2) assess actions from selected sector risk management agencies (SRMA) to enhance the cybersecurity of their sectors' IoT and OT environments;¹ and (3) identify leading guidance for addressing IoT cybersecurity, and determine the status of the Office of Management and Budget's (OMB) process for waiving cybersecurity requirements for IoT devices.

To address the first objective, we obtained and described overall IoT and OT cybersecurity initiatives or guidance from agencies, including National Institute of Standards and Technology (NIST), Department of Homeland Security (DHS) and its Cybersecurity and Infrastructure Security Agency (CISA), and OMB. Examples of guidance included NIST's *IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements* from 2021, NIST's *Guide to Industrial Control Systems (ICS) Security*, and DHS security tips on securing the Internet of Things.² We also obtained and described projects, efforts, and reports related to the cybersecurity of IoT and OT technologies from NIST's National Cybersecurity Center of Excellence and IoT working group and advisory board and the President's National Security Telecommunications Advisory Committee. In addition, we obtained and described updates and changes that were being considered to the Federal Acquisition Regulation relevant to IoT and OT cybersecurity from the Federal Acquisition Regulatory (FAR) Council. The council consists of OMB, the Department of Defense, General Services Administration (GSA), and National Aeronautics and Space Administration (NASA). Further, we interviewed cognizant officials from NIST, DHS, CISA, OMB, GSA, and NASA to verify the information provided.

¹SRMAs lead, facilitate, and support, the security and resilience programs and associated activities of their designated critical infrastructure sector.

²National Institute of Standards and Technology, *IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements*, Special Publication 800-213 (Gaithersburg, MD:, November 2021); *Guide to Industrial Control Systems (ICS) Security*, NIST Special Publication 800-82 Revision 2, (May 2015); and Cybersecurity and Infrastructure Security Agency, *Securing the Internet of Things*, Security Tip (ST17-001), Original release date: November 16, 2017 | Last revised: November 14, 2019, available online at <https://www.cisa.gov/uscert/ncas/tips/ST17-001>.

To address the second objective, we first identified the six critical infrastructure sectors³ considered to have the greatest risk of cyber compromise in the 2018 National Cyber Strategy of the United States of America.⁴ The six selected sectors were: communications, energy, information technology, healthcare and public health, financial services, and transportation systems sectors.

We then met with officials from SRMAs for each sector and with industry representatives⁵ from sector coordinating councils (SCC)⁶ and Information Sharing and Analysis Centers (ISAC)⁷ for the respective sectors and subsectors to determine the extent to which IoT and OT devices are used within their sector. Using this information, we then selected the energy, healthcare and public health, and transportation systems sectors for further review. These sectors use IoT, OT, or both types of devices extensively.⁸

³The term “critical infrastructure” refers to 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 matters. 42 U.S.C. § 5195c(e). Federal policy identifies 16 critical infrastructure sectors: chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; healthcare and public health; information technology; nuclear reactors, materials and waste; transportation systems; and water and wastewater systems.

⁴The White House, *National Cyber Strategy of the United States of America* (Washington, D.C.: September 2018).

⁵Industry representatives are from companies (both for profit and nonprofit), businesses, or bodies such as those within a critical infrastructure sector that are free from direct governmental control (e.g., SCC or ISAC representatives).

⁶Sector coordinating councils (SCC) are formed as self-organized, self-governing councils that enable critical infrastructure owners and operators, their trade associations, and other industry representatives to interact on a wide range of sector-specific strategies, policies, and activities. The SRMAs and the SCCs coordinate and collaborate in a voluntary fashion on issues pertaining to their respective critical infrastructure sectors.

⁷Information Sharing and Analysis Centers (ISAC) are sector-based organizations with the purpose of maximizing information flow between private critical infrastructure entities and the government in order to better protect entities from cyber and physical security threats.

⁸We excluded financial services, communications, and the IT sectors. The SRMA for the financial services sector reported that IoT and OT is not used within the sector. In addition, SRMA for the communications and IT sector stated that although both sectors may use IoT and OT, these devices are not critical to their operations.

Given the number of subsectors within the transportation systems sector, we interviewed Transportation officials and reviewed documentation such as the 2020 Biennial National Strategy for Transportation Security⁹ to determine if IoT and OT are critical in supporting the various subsectors.¹⁰ Using the information collected, we selected the aviation and maritime transportation systems subsectors because both reported use of IoT and OT devices in their respective subsectors and randomly selected the mass transit and passenger rail subsector from the remaining subsectors.¹¹

For the three selected sectors, we collected and evaluated documentation on IoT and OT cybersecurity efforts led by the SRMAs or sector coordinating councils. We then compared these efforts to requirements and best practices outlined in the National Defense Authorization Act (NDAA) for Fiscal Year 2021,¹² Presidential Policy Directive 21,¹³ DHS's National Plan¹⁴ and Critical Infrastructure Risk Management Framework,¹⁵ and NIST publications, such as NIST special publication *IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements*.¹⁶ We did this to determine if the selected SRMAs had cybersecurity-related processes in place to manage cybersecurity risks to IoT and OT devices for their sectors. We interviewed relevant SRMA officials to verify the information provided. We also met with industry representatives from the SCCs and

⁹Transportation Security Administration, *2020 Biennial National Strategy for Transportation Security: Report to Congress* (May 29, 2020).

¹⁰The transportation systems sector is comprised of 7 subsectors: aviation, highway and motor carrier, maritime transportation systems, mass transit and passenger rail, pipeline systems, freight rail, and postal and shipping.

¹¹We eliminated postal and shipping from our selection, as the subsector did not present any known level of use of IoT or OT.

¹²William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Publ. L. No. 116-283 § 9204, 134 Stat. 3388, 4797 (Jan. 1, 2021).

¹³The White House, *Presidential Policy Directive 21: Critical Infrastructure Security and Resilience* (Washington, D.C.: Feb. 12, 2013).

¹⁴Department of Homeland Security, *National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience* (2013).

¹⁵Department of Homeland Security, *Supplemental Tool: Executing A Critical Infrastructure Risk Management Approach*.

¹⁶National Institute of Standards and Technology, *IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements*, Special Publication 800-213 (Gaithersburg, MD: November 2021).

ISACs for the respective sectors to obtain their perspectives on challenges with managing cybersecurity vulnerabilities associated with the use of IoT and OT devices.

To address the third objective, we interviewed cognizant NIST and DHS officials as well as GSA and NASA from the Federal Acquisition Regulatory Council to determine if they had developed best practices for procurement of IoT devices. We then reviewed and described current IoT procurement best practices. We also interviewed cognizant OMB officials to determine and describe the status of the waiver development process and steps to complete it.

We conducted this performance audit from September 2021 to December 2022 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: National Institute of Standards and Technology Publications and Guidance on Internet of Things and Operational Technology

Among other responsibilities, the National Institute of Standards and Technology (NIST) is responsible for developing standards and guidelines that include minimum information security requirements for federal agencies. Table 10 includes a list of NIST’s publications and guidance related to the Internet of Things (IoT) and operational technology (OT).

Table 10: National Institute of Standards and Technology (NIST) Publications and Guidance on the Internet of Things and Operational Technology

Publication	Release Date	Description
Special Publication (SP) 800-82 Revision 2, <i>Guide to Industrial Control Systems (ICS) Security</i>	May 2015	This document provides guidance on how to secure Industrial Control Systems (ICS), including Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems, and other control system configurations such as Programmable Logic Controllers, while addressing their unique performance, reliability, and safety requirements. The document provides an overview of ICS and typical system topologies, identifies typical threats and vulnerabilities to these systems, and provides recommended security countermeasures to mitigate the associated risks. Revision 3 of this publication is pending.
SP 800-82 Revision 3 (Draft), <i>Guide to Operational Technology (OT) Security</i>	April 2022 Commenting period 4/26/22 – 7/1/22	Expands the scope of SP 800-82 to include OT, not just ICS. Describes the application of the NIST Risk Management Framework and Cybersecurity Framework to OT, and provides an overlay of the NIST SP 800-53 Revision 5a control catalog to further help organizations apply the NIST controls to OT.
Interagency Report (IR) 8089, <i>An Industrial Control System Cybersecurity Performance Testbed</i>	November 2015	NIST developed a cybersecurity performance testbed for industrial control systems. The goal of the testbed is to measure the performance of industrial control systems (ICS) when instrumented with cybersecurity controls in accordance with the best practices and requirements prescribed by national and international standards and guidelines.
IR 8188, <i>Key Performance Indicators for Process Control System Cybersecurity Performance Analysis</i>	August 2017	NIST constructed a testbed to measure the performance impact induced by cybersecurity technologies on Industrial Control Systems (ICS). The focus of this report is the Process Control System of the Testbed, which emulate an industrial continuous manufacturing system. Continuous manufacturing is a process to manufacture, produce, or process materials without interruption, the materials being processed are continuously in motion, undergoing chemical reactions or subject to mechanical or heat treatment. Examples of continuous manufacturing include chemical production, oil refining, natural gas processing, and wastewater treatment process.
IR 8227, <i>Manufacturing Profile Implementation Methodology for a Robotic Workcell</i>	May 2019	NIST constructed a testbed to measure the performance impact of cybersecurity technologies on Industrial Control Systems (ICS). The testbed was chosen to support the implementation of the Cybersecurity Framework Manufacturing Profile. This report focuses on the Collaborative Robotics System, one of the two manufacturing systems within the testbed. A methodology for implementation of technical solutions to meet the Profile language is described, as well as a comprehensive review of the testbed measurement systems, and the comparative analysis procedures used for identifying performance impacts. Finally, an example comparative analysis is performed and the characterization of the workcell is discussed.

**Appendix II: National Institute of Standards
and Technology Publications and Guidance on
Internet of Things and Operational Technology**

Publication	Release Date	Description
IR 8228, <i>Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks</i>	June 2019	The purpose of this publication is to help federal agencies and other organizations better understand and manage the cybersecurity and privacy risks associated with their individual IoT devices throughout the devices' lifecycles. It identifies considerations that may affect the management of cybersecurity and privacy risks for IoT devices as compared to conventional IT devices, identifies risk mitigation goals, and describes ways that organizations can mitigate IoT cybersecurity and privacy risks.
IR 8183 Revision 1, <i>Cybersecurity Framework Version 1.1 Manufacturing Profile</i>	October 2020	This document provides the Cybersecurity Framework Version 1.1 implementation details developed for the manufacturing environment. The "Manufacturing Profile" of the Framework can be used as a roadmap for reducing cybersecurity risk for manufacturers that is aligned with manufacturing sector goals and industry best practices. This Manufacturing Profile provides a voluntary, risk-based approach for managing cybersecurity activities and reducing cyber risk to manufacturing systems. NIST also published three companion publications providing more specific implementation guidance for the Manufacturing Profile
IR 8259, <i>Foundational Cybersecurity Activities for IoT Device Manufacturers</i>	May 2020	This publication describes recommended activities related to cybersecurity that manufacturers should consider performing before their IoT devices are sold to customers. These foundational cybersecurity activities can help manufacturers lessen the cybersecurity-related efforts needed by customers, which in turn can reduce the prevalence and severity of IoT device compromises and the attacks performed using compromised devices.
IR 8259A, <i>IoT Device Cybersecurity Capability Core Baseline</i>	May 2020	This publication defines an Internet of Things (IoT) device cybersecurity capability core baseline, which is a set of device capabilities generally needed to support common cybersecurity controls that protect an organization's devices as well as device data, systems, and ecosystems. The purpose of this publication is to provide organizations a starting point to use in identifying the device cybersecurity capabilities for new IoT devices they will manufacture, integrate, or acquire. It may be used in conjunction with NIST IR 8259.
Draft IR 8259D, <i>Profile Using the IoT Core Baseline and Non-Technical Baseline for the Federal Government</i>	December 2020 (Commenting period: 12/15/20-02/26/21)	The NISTIR 8259 series provide general guidance on how manufacturers can understand and approach their role in supporting customers' cybersecurity needs and goals. As discussed in those documents, specific sectors and use cases may require more specific guidance than what is included in the device capability core baseline in NISTIR 8259A and the non-technical and supporting capability baseline in NISTIR 8259B for IoT devices. This publication provides the profile created for the federal government using the process described in NISTIR 8259C, which can serve as a helpful starting point in determining and anticipating federal agencies' IoT device cybersecurity requirements.
Draft IR 8259C, <i>Creating a Profile Using the IoT Core Baseline And Non-Technical Baseline</i>	December 2020 (Commenting period: 12/15/20-02/26/21)	Draft NISTIR 8259C describes a process, usable by any organization, that starts with the core baselines provided in NISTIRs 8259A and 8259B and explains how to integrate those baselines with organization- or application-specific requirements (e.g., industry standards, regulatory guidance) to develop a IoT cybersecurity profile suitable for specific IoT device customers or applications. The process in NISTIR 8259C guides organizations needing to define a more detailed set of capabilities responding to the concerns of a specific sector, based on some authoritative source such as a standard or other guidance, and could be used by organizations seeking to procure IoT technology or by manufacturers looking to match their products to customer requirements.

**Appendix II: National Institute of Standards
and Technology Publications and Guidance on
Internet of Things and Operational Technology**

Publication	Release Date	Description
IR 8259B, <i>IoT Non-Technical Supporting Capability Core Baseline</i>	August 2021	This publication defines an Internet of Things (IoT) device manufacturers' non-technical supporting capability core baseline, which is a set of non-technical supporting capabilities generally needed from manufacturers or other third parties to support common cybersecurity controls that protect an organization's devices as well as device data, systems, and ecosystems. The purpose of this publication is to provide organizations a starting point to use in identifying the non-technical supporting capabilities needed in relation to IoT devices they will manufacture, integrate, or acquire. It is intended to be used in conjunction with NISTIR 8259, <i>Foundational Cybersecurity Activities for IoT Device Manufacturers</i> and NISTIR 8259A, <i>IoT Device Cybersecurity Capability Core Baseline</i>
SP 800-213, <i>IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements</i>	November 2021	This publication contains background and recommendations to help organizations consider how an IoT device they plan to acquire can integrate into a system. IoT devices and their support for security controls are presented in the context of organizational and system risk management. This publication provides guidance on considering system security from the device perspective. This allows for the identification of device cybersecurity requirements—the abilities and actions an organization will expect from an IoT device and its manufacturer or third parties, respectively.
SP 800-213A, <i>IoT Device Cybersecurity Guidance for the Federal Government: IoT Device Cybersecurity Requirement Catalog</i>	November 2021	This publication provides a catalog of Internet of Things (IoT) device cybersecurity capabilities and non-technical supporting capabilities that can help organizations as they use SP 800-213 to determine and establish device cybersecurity requirements.

Source: GAO summary of NIST documentation | GAO-23-105327

NIST established the National Cybersecurity Center of Excellence (NCCoE) in 2012 in partnership with the state of Maryland and with Montgomery County, Maryland. Working with technology industry partners, the NCCoE develops cybersecurity solutions demonstrating how to apply standards and best practices using commercially available technology. The NCCoE documents below detail selected cybersecurity solutions (see table 11).

**Appendix II: National Institute of Standards
and Technology Publications and Guidance on
Internet of Things and Operational Technology**

Table 11: National Institute of Standards and Technology (NIST) National Cybersecurity Center of Excellence (NCCoE) Publications on the Cybersecurity of Internet of Things (IoT) and Operational Technology (OT) Devices

Publication	Release date	Description
Special Publication (SP) 1800-2, <i>Identity and Access Management for Electric Utilities</i>	July 2018	NCCoE developed an example solution that electric utilities can use to more securely and efficiently manage access to the networked devices and facilities on which power generation, transmission, and distribution depend. This Cybersecurity Practice Guide uses commercially available products that can be included alongside current products in an electric utility's existing infrastructure. The integration of these products provides a converged view of all users within the electric utility's operational technology (OT) systems and IT systems, as well as access to buildings and other facilities.
SP 1800-7, <i>Situational Awareness for Electric Utilities</i>	August 2019	This NIST Cybersecurity Practice Guide demonstrates how organizations can use commercially available products that can be integrated with an organization's existing infrastructure. The combination of these products provides a converged view of all sensor data within the utility's network systems, including IT, operational, cyber, and physical access control systems, which often exists in separate "silos." The example solution is packaged as a "how to" guide that demonstrates implementation of standards-based cybersecurity technologies in the real world and based on risk management. The guide may help inform electric utilities in their efforts to gain situational awareness efficiencies.
SP 1800-23, <i>Energy Sector Asset Management For Electric Utilities, Oil & Gas Industry</i>	May 2020	The NCCoE, in collaboration with experts from the energy sector and technology vendors, developed an asset management example solution that includes managing, monitoring, and baselining OT assets to reduce the risk of cybersecurity incidents. This practice guide outlines practical steps on how organizations can implement new asset management capabilities or leverage existing asset management capabilities, to enhance the security of OT assets.
NIST IR 8219, <i>Securing Manufacturing Industrial Control Systems: Behavioral Anomaly Detection</i>	July 2020	Capabilities enable manufacturers to detect anomalous conditions in their operating environments to mitigate malware attacks and other threats to the integrity of critical operational data. NIST has mapped these demonstrated capabilities to the Cybersecurity Framework and have documented how this set of standards-based controls can support many of the security requirements of manufacturers. This report documents the use of behavioral anomaly detection capabilities in two distinct but related demonstration environments: a robotics-based manufacturing system and a process control system that resembles what is being used by chemical manufacturing industries.
SP 1800-15, <i>Securing Small-Business and Home Internet of Things (IoT) Devices: Mitigating Network-Based Attacks Using Manufacturer Usage Description (MUD)^a</i>	May 2021	This NIST Cybersecurity Practice Guide explains how MUD protocols and tools can reduce the vulnerability of IoT devices to botnets and other network-based threats as well as reduce the potential for harm from exploited IoT devices. It also shows IoT device developers and manufacturers, network equipment developers and manufacturers, and service providers who employ MUD-capable components how to integrate and use MUD to satisfy IoT users' security requirements.
NIST IR 8349 (Draft), <i>Methodology for Characterizing Network Behavior of Internet of Things Devices</i>	January 2022	This draft publication demonstrates how to use device characterization techniques and a supporting open source tool developed by the NCCoE to describe the communication requirements of IoT devices. Manufacturers and network administrators can use the techniques and tools described in the report for capturing network communications from IoT devices and analyzing network captures to help ensure IoT devices perform as intended.

**Appendix II: National Institute of Standards
and Technology Publications and Guidance on
Internet of Things and Operational Technology**

Publication	Release date	Description
SP 1800-32, <i>Securing Distributed Energy Resources: An Example of Industrial Internet of Things Cybersecurity</i>	February 2022	Protecting Industrial Internet of Things (IIoT) devices at the grid edge is arguably one of the more difficult tasks in cybersecurity. There is a wide variety of devices, many of which are deployed and operate in a highly specific manner. Their connectivity, the conduit through which they can become vulnerable, represents a growing cyber threat to the distribution grid. In this practice guide, the NCCoE applies standards, best practices, and commercially available technology to protect the digital communication, data, and control of cyber-physical grid-edge devices. The publication demonstrates how to monitor and detect unusual behavior of connected IIoT devices and build a comprehensive audit trail of trusted IIoT data flows.
SP 1800-10, <i>Protecting Information and System Integrity in Industrial Control System Environments: Cybersecurity for the Manufacturing Sector</i>	March 2022	This cybersecurity practice guide summarizes the results of a project in which NIST built example solutions that manufacturing organizations can use to mitigate ICS integrity risks, strengthen the cybersecurity of OT systems, and protect the data that these systems process.

Source: GAO summary of NIST NCCoE documentation | GAO-23-105327

^aThe goal of the Internet Engineering Task Force's Manufacturer Usage Description (MUD) specification is for IoT devices to behave as the devices' manufacturers intended. MUD provides a standard way for manufacturers to indicate the network communications that a device requires to perform its intended function. When MUD is used, the network will automatically permit the IoT device to send and receive only the traffic it requires to perform as intended, and the network will prohibit all other communication with the device, thereby increasing the device's resilience to network-based attacks.

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

November 16, 2022

Dave Hinchman
Acting Director, Information Technology
and Cybersecurity
U.S. Government Accountability Office
441 G Street NW
Washington, DC 20548

Dear Mr. Hinchman:

Attached are comments on the U.S. Government Accountability Office's (GAO) report entitled, "**Critical Infrastructure: Actions Needed to Better Secure Internet-Connected Devices**" (GAO-23-105327).

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 FROM THE DEPARTMENT OF HEALTH & HUMAN SERVICES
ON THE GOVERNMENT ACCOUNTABILITY OFFICE'S DRAFT REPORT ENTITLED —
CRITICAL INFRASTRUCTURE - ACTIONS NEEDED TO BETTER SECURE INTERNET -
CONNECTED DEVICES (GAO-23-105327)**

Recommendation 3: The Secretary of Health and Human Services, as SRMA for the healthcare and public health sector, should direct the Assistant Secretary for Preparedness and Response to use the National Plan to develop a sector-specific plan that includes metrics for measuring the effectiveness of their efforts to enhance the cybersecurity of their sectors' IoT and OT environments.

HHS response:

ASPR plans to update the Sector Specific Plan once the National Plan is released. However, some challenges that ASPR faces are that ASPR alone does not have the authorities or resources to track the implementation or success of the plan as it related to IOT and OT outside of medical devices across the sector as the IoT and OT landscape outside of medical devices are extremely vast, not specific to healthcare and crosses multiple disciplines and critical infrastructures. Additionally, ASPR cannot compel adoption of the plan in the private sector. HHS will continue to consult and coordinate with ASPR, other relevant HHS offices, and other federal agencies such as DHS/CISA and DOC/NIST, while reviewing this recommendation and considering the development of metrics.

Recommendation 4: The Secretary of Health and Human Services, as SRMA for the healthcare and public health sector, should direct the Assistant Secretary for Preparedness and Response to include IoT and OT devices as part of the risk assessments of its sectors cyber environment.

HHS Response:

Currently ASPR has 1.5 FTE committed to the SRMA mission and performs contextual risk assessments, identifying interdependencies between cybersecurity and all-hazards incidents. ASPR currently communicates identified cybersecurity vulnerabilities, threats, and mitigation strategies to the HPH sector, reaching over 3,800 partners through recurring newsletters. While ASPR does not have the capacity for an additional mission in IoT outside of medical devices, ASPR will continue to rely heavily on partners within HHS, the 405d program and the Healthcare Cyber Coordination Center (HC3), and external partners to execute these broad cybersecurity responsibilities. ASPR takes a holistic approach to these responsibilities and will continue its risk assessment efforts.

As referenced in the response to recommendation three, HHS will continue to consult and coordinate with ASPR, other relevant HHS offices, and other federal agencies such as DHS/CISA and DOC/NIST while reviewing this recommendation.

Appendix IV: Comments from the Department of Homeland Security

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



**Homeland
Security**

November 10, 2022

David Hinchman
Acting Director, Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Re: Management Response to Draft Report GAO-23-105327, "CRITICAL INFRASTRUCTURE: Actions Needed to Better Secure Internet-Connected Devices"

Dear Mr. Hinchman:

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 Transportation Security Administration's (TSA) and U.S. Coast Guard's roles as executive agents for the Transportation Systems Sector (TSS) and the efforts to issue cybersecurity guidance and appoint cybersecurity coordinators. DHS remains committed to protecting critical infrastructure from cybersecurity-related threats, especially those threats to Operational Technology (OT) systems and networks, such as through TSA-issued security directives and security program amendments. This guidance places a special emphasis on requiring TSS stakeholders to develop performance-based cybersecurity measures that implement network segmentation policies and controls designed to prevent operational disruption to the OT system if the Information Technology (IT) system is compromised, or to the IT system if the OT system is compromised.

The draft report contained nine recommendations, including two for DHS with which the Department concurs. Enclosed find our detailed response to each recommendation. DHS previously submitted technical comments addressing accuracy, contextual, and other issues under a separate cover for GAO's consideration.

**Appendix IV: Comments from the Department
of Homeland Security**

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: 2022.11.10 13:43:48 -05'00'

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

Enclosure

**Enclosure: Management Response to Recommendations
Contained in GAO-23-105327**

GAO recommended that the Secretary of Homeland Security direct the TSA Administrator and the Commandant of the Coast Guard to:

Recommendation 5: Jointly work with the Department of Transportation’s Office of Intelligence, Security and Emergency Response, as co-SRMAs [Sector Risk Management Agencies] for the transportation systems sector, to use the National Plan to develop a sector-specific plan that includes metrics for measuring the effectiveness of their efforts to enhance the cybersecurity of their sector’s IoT [Internet of Things] and OT environments.

Response: Concur. TSA’s Office of Strategy, Policy Coordination and Innovation, in coordination with the Coast Guard’s Office of Port and Facility Compliance, other offices and divisions, as appropriate, and the Department of Transportation, is developing a draft sector-specific plan that will include metrics for measuring effectiveness of efforts to enhance the cybersecurity of the sector’s IoT and OT environments. As part of this effort, the “National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience,” dated December 2013 (the National Plan) is currently under review and revision. Specifically, the co-SRMAs will develop an updated sector-specific plan to leverage information in the next version of the National Plan. This effort is in the early planning stages and the co-SRMAs will need further coordination to identify a more detailed set of milestones. While a draft sector-specific plan is anticipated to be ready for leadership clearance in six to eight months, full implementation of these actions are contingent on the issuance of the revised National Plan. Estimated Completion Date (ECD): To Be Determined

Recommendation 6: Jointly work with the Department of Transportation’s Office of Intelligence, Security and Emergency Response, as co-SRMAs for the transportation systems sector to include IoT and OT devices as part of the risk assessments of its sectors cyber environment.

Response: Concur. TSA’s Office of Risk Assessment and Analysis has incorporated cybersecurity issues (including consideration of OT and IoT) in the Transportation Systems Sector Risk Assessment (TSSRA)¹ 8.0, dated August 20, 2021, and will continue efforts to include IOT and OT devices in risk assessments. ECD: June 28, 2024

¹ The TSSRA is a broad, high-level scenario-based terrorism risk assessment that looks across TSA’s mission area, including aviation, mass transit and passenger rail, highway and motor carriers, pipelines, and freight rail. The TSSRA is Sensitive Security Information, and not publicly available. TSSRA 8.0 was approved on August 20, 2021.

Appendix V: GAO Contact and Staff Acknowledgments

GAO Contact

David B. Hinchman at (214) 777-5719, hinchmand@gao.gov

Staff Acknowledgments

In addition to the contact named above, Neela Lakhmani (Assistant Director), Kara Lovett Epperson (Analyst-in-Charge), Brottie Barlow, Christopher Businsky, William Cook, Vijay A. D'Souza, Donna Epler, Douglas Harris, and Jonah Silencieux made significant 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



Please Print on Recycled Paper.