United States Government Accountability Office

Congressional Requesters

August 2020

INTERNET OF THINGS

Information on Use by Federal Agencies

GAO-20-577

GAO Highlights

Highlights of GAO-20-577, a report to congressional requesters

August 2020

INTERNET OF THINGS

Information on Use by Federal Agencies

Why GAO Did This Study

IoT generally refers to devices—from sensors in vehicles to building thermostats— that collect information, communicate it to a network, and may complete a task based on that information. Although IoT technologies may present an opportunity for the federal government to operate more efficiently and effectively, federal agencies may also face challenges in acquiring and using IoT.

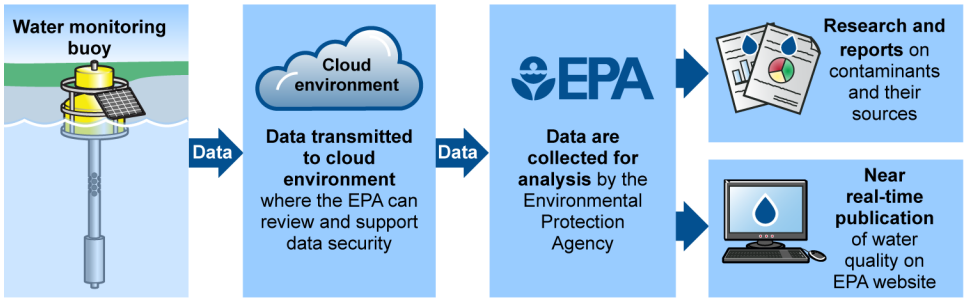
GAO was asked to review the federal government's experience with IoT. This report describes (1) IoT technologies selected federal agencies are using, (2) the benefits and challenges of using IoT technologies, and (3) policies and guidance selected agencies follow in using and acquiring IoT technologies. GAO surveyed 115 Chief Information Officers (CIO) and senior IT officials at federal agencies and subcomponents based on, in part, agency membership in the federal CIO Council; 90 responded. However, not all agencies replied to each question. GAO also selected the Department of Commerce, the Department of Homeland Security, EPA, and the National Aeronautics and Space Administration as case studies. GAO selected these agencies based on, among other things, their fiscal year 2020 IT budgets and examples of IoT use from literature. For each case study, GAO reviewed documents and interviewed officials from the Office of the CIO from the agency and officials from selected sub-components that use the IoT technologies.

View GAO-20-577. For more information, contact Andrew Von Ah at (202) 512-2834 or vonaha@gao.gov.

What GAO Found

Many federal agencies (56 of 90) responding to GAO's survey reported using Internet of Things (IoT) technologies. Most often, agencies reported using IoT to: (1) control or monitor equipment or systems (42 of 56); (2) control access to devices or facilities (39 of 56); or (3) track physical assets (28 of 56) such as fleet vehicles or agency property. Agencies also reported using IoT devices to perform tasks such as monitoring water quality, watching the nation's borders, and controlling ships in waterway locks. Furthermore, IoT use by federal agencies may increase in the future, as many agencies reported planning to begin or expand the use of IoT. However, 13 agencies not using IoT technologies reported they did not plan to use the technologies for a range of reasons, including insufficient return on investment.

Example of Government's Use of Internet of Things Technology: Environmental Protection Agency's (EPA) Water Monitoring Buoy



Sources: GAO and EPA. | GAO-20-577

Surveyed agencies most frequently reported increasing data collection (45 of 74), and increasing operational efficiency (43 of 74) as benefits of using IoT technologies. Increasing data collection can aid decision-making and support technology development; increased efficiencies may allow agencies to accomplish more with existing resources. According to EPA officials, sensors are able to transmit data eliminating the need for employees to visit sites to collect data. The Saint Lawrence Seaway Development Corporation reported that IoT technologies helped improve transit times through its locks. Agencies most frequently reported cybersecurity issues (43 of 74) and interoperability (30 of 74) as the most significant challenges to adopting IoT technologies. For example, the Transportation Security Administration's officials told us they could not ensure the security and privacy of passenger information and subsequently took its network-connected security equipment offline until they developed a solution.

Most agencies' officials responding to GAO's survey (54 of 72), as well as officials interviewed as part of the case studies, reported using information technology (IT) policies developed by their agency, versus internal IoT-specific policies, to manage IoT technologies. Some agencies reported their IT policies were sufficient for the current challenges and risks associated with adopting IoT technologies, including cybersecurity. The Office of Management and Budget's officials stated they do not typically make policies for specific IT components but if needed would work with the National Institute of Standards and Technology and others to develop such policies.

Contents

Abbreviations

AST	Autonomous Surveillance Tower
CBP	Customs and Border Protection
CIO	Chief Information Officer
Commerce	Department of Commerce
DHS	Department of Homeland Security
DOD	Department of Defense
EPA	Environmental Protection Agency
FISMA	Federal Information Security Modernization Act of 2014
FITARA	Federal Information Technology Acquisition Reform Act
GCC	Government Coordinating Councils
GSA	General Services Administration
IoT	Internet of Things
IT	information technology
NASA	National Aeronautics and Space Administration
NIST	National Institute of Standards and Technology
NTIA	National Telecommunications and Information Administration
OMB	Office of Management and Budget
SCC	Sector Coordinating Council
Seaway	St. Lawrence Seaway
SLSDC	Saint Lawrence Seaway Development Corporation

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

August 13, 2020

The Honorable Brian Schatz
Ranking Member
Subcommittee on Communications,
Technology, Innovation, and the Internet
Committee on Commerce, Science,
and Transportation
United States Senate

The Honorable Deb Fischer
United States Senate

The Honorable Cory Gardner
United States Senate

The Honorable Cory Booker
United States Senate

The Internet of Things (IoT) 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. The growth of IoT in the private sector has continued in recent years, and the worldwide numbers of devices are predicted to increase to 43 billion by 2023.[1] With respect to federal government use, a 2016 report found that although IoT technologies present an opportunity for the federal government to operate more efficiently and effectively, federal agencies may face challenges in acquiring and using IoT technologies.[2] Our prior work indicated these challenges can include issues about the security and privacy of the network that the technologies communicate across and the data captured by these technologies.[3] In 2017, we reported on two challenges faced by

[1]McKinsey & Company, Growing Opportunities in the Internet of Things (July 2019).

[2]D. Castro, J. New, and A. McQuinn, *How Is the Federal Government Using the Internet of Things?* (Washington, D.C.: Center for Data Innovation, July 25, 2016).

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

the Department of Defense due to IoT technologies, security risks, and associated policy gaps.[4]

Nonetheless, the 2016 report found that some federal agencies had implemented IoT technologies, either to reduce costs (for example, energy and vehicle maintenance costs) or to create new services, such as environmental monitoring and improved disaster response.[5] Federal agencies have also used IoT technologies to support building operations. In 2018, we reported that the General Services Administration (GSA) implemented IoT technologies as part of its "Smart Buildings" program, in part, to monitor connected heating and cooling systems and measure utility consumption in real-time.[6]

You asked us to review federal agencies' current use and experience with IoT technologies. This report addresses:

- IoT technologies that selected federal agencies are using,
- benefits and challenges agencies associated with using IoT technologies, and
- federal policies and guidance that inform agencies' decision-making about using and acquiring IoT technologies.

To describe the IoT technologies federal agencies are using, the benefits and challenges of the technologies, and the policies and guidance that inform agencies' decision-making about using and acquiring IoT technologies, we sent a survey to 115 Chief Information Officers (CIO) and senior information technology officials at selected federal agencies and sub-components. We surveyed federal agencies and sub-components that were members of the Federal CIO Council. For larger agencies, we selected sub-component organizations within the relevant agencies that were classified as an administration, agency, authority, bureau, center, corporation, institute, or service in order to identify a selected number of sub-components that would be able to speak to IoT

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

[5]Castro, New, and McQuinn, *How Is the Federal Government Using the Internet of Things?*

[6]GAO, *Federal Buildings: GSA Should Establish Goals and Performance Measures to Manage the Smart Buildings Program*, GAO-18-200 (Washington, D.C.: Jan. 30, 2018). This report included recommendations for GSA to establish clearly defined performance goals and related measures for the smart buildings program, and identify and develop data to measure progress. GSA implemented both recommendations.

use. For smaller federal agencies, we surveyed the CIOs of the top-level of the organization because they do not have any subordinate components that meet the above criteria. We pre-tested our survey questionnaire with three federal CIOs or senior information technology (IT) executives to check: (1) that the questions were clear and unambiguous, (2) that terminology was used correctly, (3) that the questionnaire did not place an undue burden on agency officials, (4) that the information could feasibly be obtained, and (5) that the survey was comprehensive and unbiased.

We conducted the web-based survey from December 16, 2019, to February 12, 2020, and received 90 survey responses resulting in a 78 percent response rate. However, not all agencies responded to every question, and so, throughout the report, the total responses vary. For a copy of the survey responses and a list of the federal agencies and sub-components we surveyed, see appendixes I and II, respectively. When discussing the survey results in this report, there are occasions we use the terms “some,” “many,” and “most”. For the purposes of reporting these survey results, “some” refers to a quantity of one-third or fewer of a question’s responses; “many” refers to refers to a quantity of responses between one-third and two-thirds; and “most” refers to quantities that are two-thirds or greater of a question’s total responses.

To learn more about how agencies are using IoT technologies, the benefits and challenges they experience, and the policies and guidance they use, we also selected four case study agencies from the Federal CIO Council. The selection was based on three criteria: the agencies’ fiscal year 2020 budget for information technology, use case examples found in literature, and the mission of the agencies. To include a mix of larger agencies and smaller agencies, we chose three agencies with fiscal year 2020 IT budgets over $1 billion, and one agency whose fiscal year 2020 IT budget was under $1 billion. We also narrowed the field of case study agencies based on examples of IoT use identified through a literature review. We did this to provide assurance that the agencies we included had experience using IoT technologies in support of their missions. The last criterion was that our agencies reflect a variety of missions to include at least one agency with a security mission and one with a science mission. As a result of applying these criteria, we selected the Department of Commerce (Commerce); the Department of Homeland Security (DHS); the Environmental Protection Agency (EPA); and the National Aeronautics and Space Administration (NASA) as our case study agencies. For each case study, we reviewed documents and interviewed

staff from the Office of the CIO from the agency and staff from selected sub-components that use the IoT technologies.[7]

We also reviewed laws related to IoT, such as the Federal Information Technology Acquisition Reform Act (FITARA)[8] and the Federal Information Security Modernization Act of 2014 (FISMA),[9] and interviewed officials at the Office of Management and Budget (OMB); National Institute of Standards and Technology (NIST); and the National Telecommunications and Information Administration (NTIA). For more information on our scope and methodology, see Appendix III.

We conducted this performance audit from May 2019 to July 2020 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

IoT Technologies

Versions of networked objects have existed for decades; however, as we reported in 2017, recent technological advances in IoT components have accelerated the development of IoT technologies. These technologies consist of three primary components—hardware, network connectivity, and software that interact to complete tasks.[10] The tasks can be

[7]We interviewed and reviewed documents from the following sub-components of the case study agencies: Ames Research Center (NASA); Customs and Border Protection (DHS); Cybersecurity and Infrastructure Security Administration (DHS); Johnson Space Center (NASA), Langley Research Center (NASA); National Oceanic and Atmospheric Administration (Commerce); Office of Land and Emergency Management (EPA); Office of Water (EPA); Science and Technology Directorate (DHS); and Transportation Security Administration (DHS).

[8]FITARA was enacted into law as part of the Carl Levin and Howard P. 'Buck' McKeon National Defense Authorization Act of 2015. Pub. L. No. 113-291, div. A, title VIII, subtitle D, 128 Stat. 3292, 3438-50 (2014) (codified at 40 U.S.C. §§ 11302, 11319, 11331, & 44 U.S.C. § 3601).

[9]Pub. L. No. 113-283, 128 Stat. 3073 (2014) (codified at 44 U.S.C. §§ 3551-58).

[10]GAO-17-75.

completed through pre-programmed responses or are based on the device learning responses.

- **Hardware.** The hardware component consists of sensors, actuators, and processors, among other components. Sensors collect information such as temperature or motion. Actuators perform physical actions such as unlocking or opening a door. Processors serve as the "brains" of IoT devices, supporting the computing platform for the network and software components and interfacing with the sensors and actuators. Recently, the hardware components have advanced to include more features—such as, miniaturized and inexpensive electronics—making it easier for designers and manufacturers to embed the hardware into objects, like a refrigerator, enabling them as IoT devices.
- **Network.** The network component of IoT devices is used to connect to other IoT devices or computer systems. IoT devices connect via wireless and wired connections. Wireless devices typically connect via the radio frequency spectrum, often using Bluetooth and Wi-Fi for short-range wireless connections, while cellular networks can be used for long-range wireless connections.[11] The expansion of wireless networks and the decrease in the cost of deploying these networks allows for easier connectivity and allows for IoT devices to connect almost anywhere.
- **Software.** The software component in IoT devices performs a range of functions, from basic operations to complex analyses of collected data. For example, software of one IoT device may translate data from one format to another. Other software might analyze data to monitor the functionality of complex machines. The software component may also include data analytics to find patterns, correlations, or outliers, among other information, in the collected data.

Federal Agencies

Several federal agencies have responsibilities for helping oversee and guide the adoption and use of IoT technologies. OMB 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,

[11]Cellular networks are wireless telecommunications networks managed by service providers.

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.[12] OMB also noted that encouraging the use of IoT falls under its normal support of agency operations.

NIST is a physical sciences laboratory and a non-regulatory agency of the Department of Commerce. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal systems under FISMA. NIST's mission is to promote innovation and industrial competitiveness, and to provide technical leadership for federal agencies and the private sector. In the area of IoT, NIST issues technical guidance, most specifically for cybersecurity. Generally, according to NIST, its role in IoT has been to create guidelines and frameworks to provide researchers, developers, and users with a common language for approaching data, cyber-security, and privacy challenges.

DHS oversees IT-specific issues in support of the National Infrastructure Protection Plan (NIPP).[13] 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.[14]

Federal Laws

Federal laws also guide the acquisition and use of information technology, including IoT, by federal agencies. FISMA requires federal executive branch agencies to develop, document, and implement an

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

[13]DHS, *National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience* (2013). The NIPP's purpose is to guide the national effort to manage risks to the nation's critical infrastructure through developing partnerships between government and private sector entities that support critical infrastructure to identify national priorities, articulate clear goals, and mitigate risk, among other goals.

[14]DHS coordinates across the government through Government Coordinating Councils (GCC), which are aligned to various areas of critical infrastructure. DHS chairs the GCC that supports IT infrastructure and coordinates with the Sector Coordinating Council (SCC) that supports IT infrastructure. SCCs are comprised of private sector entities and similarly align to various areas of critical infrastructure.

agency-wide programs to provide information security for the information systems that support the operations and assets of the agencies, among other things.[15] The act requires program officials, and the head of each agency, to conduct annual reviews of information security programs, to determine their effectiveness.[16] Among other responsibilities, FISMA requires the head of each agency to ensure the provision of information security for the information and information systems in the agency, in order to keep risks at or below specified acceptable levels in a cost-effective, timely, and efficient manner. Furthermore, FISMA directs OMB to oversee government-wide agency information security policies and practices and DHS to administer the implementation of agencies' information security policies and practices by developing, issuing, and overseeing implementation of binding operational directives.

Similarly to FISMA, FITARA sets forth requirements, which agencies have applied to IoT technologies, for agencies to meet and follow regarding IT. FITARA provided the Chief Information Officers of certain agencies with enhanced authorities and a greater role in agencies' management and acquisition of IT and in performing risk management in major IT investments, among other things.[17] For IoT, major investments in this technology must be monitored and reported under the FITARA requirements.[18]

Many Federal Agencies Report Using IoT Technologies for a Variety of Purposes

Federal Agencies Are Using Various IoT Technologies

Many federal agencies responding to our survey reported using IoT technologies, and for a variety of purposes (see fig. 1). Specifically, 56 of 90 agencies reported using IoT technologies in at least one of eight

[15]44 U.S.C. § 3554.

[16]44 U.S.C. § 3555.

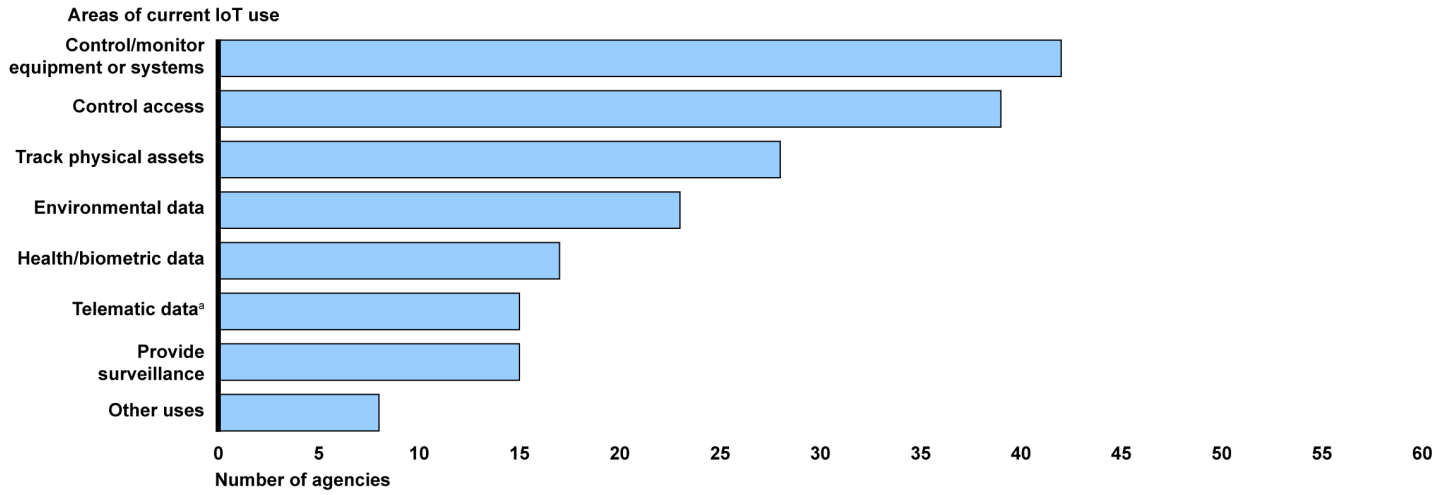
[17]Pub. L. No. 113-291, 128 Stat. 3439-40 (codified at 40 U.S.C. §11319(a)-(b)).

[18]Pub. L. No. 113-291, 128 Stat. at 3440 (codified at 40 U.S.C. §11302(c)).

areas. These agencies most frequently identified using IoT technologies in the following three areas:

- controlling or monitoring equipment or systems (42 of 56);
- controlling access to devices or facilities (39 of 56); and
- tracking physical assets (28 of 56), such as fleet vehicles or agency property.

Figure 1: Number of Federal Agencies Currently Using Internet of Things Technologies for Various Purposes



Source: GAO survey of federal agencies and sub-components. | GAO-20-577

The federal agencies' specific uses of IoT technologies varied across these different purposes. The most frequently cited purpose, controlling and monitoring equipment or systems, includes various building control systems. As previously mentioned, we reported in 2018 on GSA's smart-building technologies that are used to control and monitor the use of building utilities such as gas and electric.[19] Furthermore, our survey respondents and case study agencies identified using IoT technologies for various other purposes, as described in the examples below.

Environmental data collection:

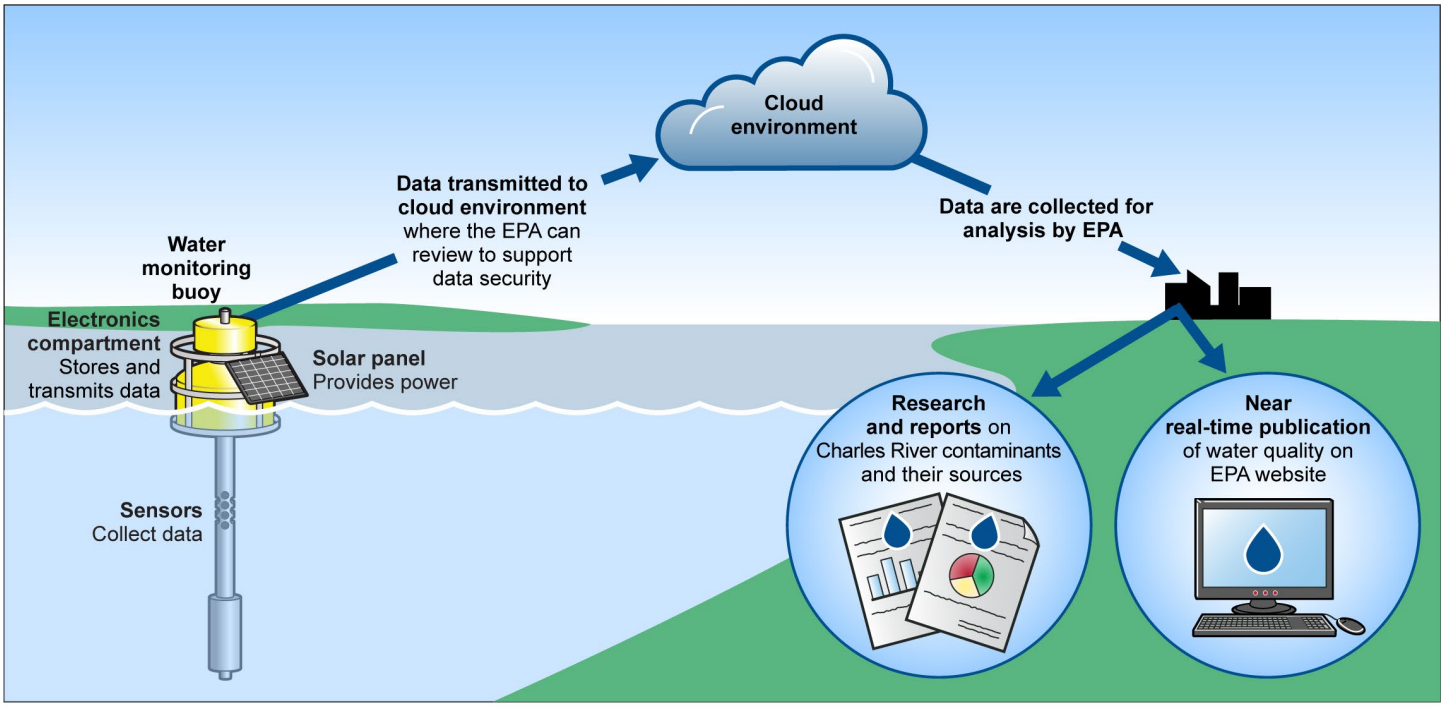
- NOAA monitors lab environments where water temperature, light, and other factors are tracked by sensors to ensure the water lab pumps

[19]GAO-18-200.

water from the ocean at high tide to keep sediment out of the lab tanks.

- EPA places various sensors on buoys in the Charles River to monitor water quality (see fig. 2). According to EPA, scientists and water quality managers use data from these sensors to monitor water temperature, pH, and oxygen levels, among other readings. Furthermore, EPA uses the sensors to monitor bacteria blooms that can be harmful to humans and fish. The data are then transmitted wirelessly for remote access on EPA's website.

Figure 2: Environmental Protection Agency (EPA) Buoy That Uses Internet of Things Technologies to Remotely Monitor Water Quality in the Charles River



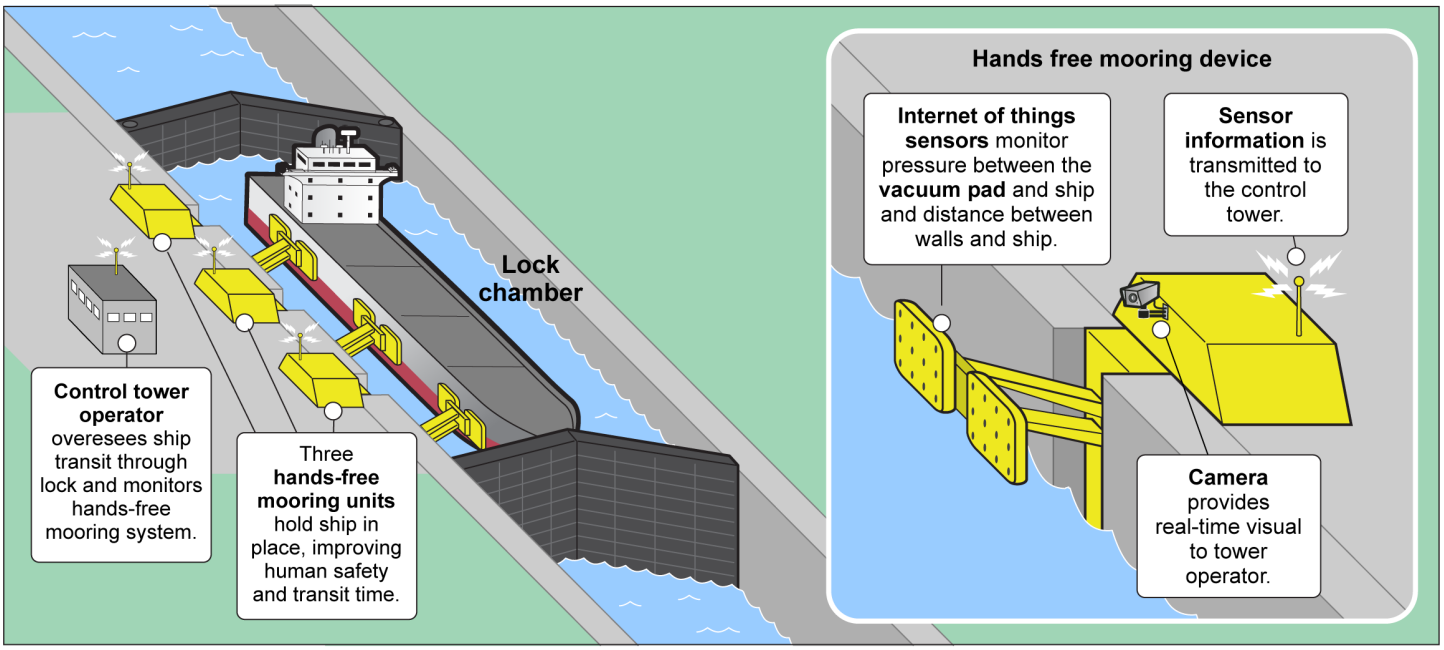
Sources: GAO and EPA. | GAO-20-577

- EPA set up sensor systems to monitor air quality during the Kilauea volcanic eruptions in 2018. Specifically, EPA deployed monitoring stations that collected data on sulfur dioxide, hydrogen sulfide, and particulates to support assessments of the threats to public health from the volcanic emissions. Overall, EPA deployed 12 monitoring stations and staff to support the data management and analysis.

Monitoring and controlling systems and equipment:

- The Saint Lawrence Seaway Development Corporation (SLSDC) implemented hands-free mooring technology at its two vessel locks throughout the St. Lawrence Seaway (Seaway).[20] According to SLSDC officials, this technology uses a series of vacuum pads that attach to commercial ships to hold them in place as they move through the locks throughout the Seaway (see fig. 3). The officials said this technology contains IoT sensors that, among other things, monitor the ships' distance from the lock walls and the forces exerted on the vacuum pads, providing real-time data to the operator. SLSDC tracks these data over time to assess performance relative to the time and number of commercial ships transiting through the locks. This IoT technology supports improved safety for workers and improved efficiencies in moving cargo throughout the Seaway.

Figure 3: Saint Lawrence Seaway Development Corporation's Hands Free Mooring System That Uses Internet of Things Sensors to Monitor and Control Ships Transiting Locks



Sources: GAO and SLSDC. | GAO-20-577

[20]A lock is a device used for raising and lowering boats, ships and other watercraft between stretches of water of different levels on river and canal waterways. The St. Lawrence Seaway has 15 locks, 2 operated by the United States SLSDC and 13 operated by its Canadian counterpart. The IoT mooring technology is installed on 13 of the 15 locks.

- NASA is conducting research on sensors for use on rockets that can identify safety issues and provide data readings at greater frequencies than previous technologies. According to NASA officials, NASA is testing IoT sensor technology on rockets using wireless technologies to improve capabilities in non-critical areas of flight. These capabilities could provide new or redundant diagnostic capabilities to provide new data readings or help resolve unclear data readings. For example, this technology was part of a test rocket and measured temperature and pressure on an external braking system and within the rockets nose cone.[21] These systems were able to provide data about the rocket from the sensors during the test flight.
- NASA officials also reported exploring the use of IoT in spacesuits to help monitor life-support functions and make critical adjustments to systems without the astronauts' input. Currently, astronauts watch monitors and adjust gauges to ensure the space suit is operating properly. However, NASA is researching combining IoT technologies and artificial intelligence to maintain the space suit during a spacewalk. Rather than the astronaut having to make adjustments to the suit during the walk, the new suit would use sensors to monitor the status of the astronaut and then automatically make adjustments. For example, according to NASA officials, if the astronaut's temperature were rising, the response might be to circulate water to cool them down.

Surveillance:

- DHS's Customs and Border Protection (CBP) uses Autonomous Surveillance Towers (AST) along the nation's southwest border to assist in securing the border from illegal entry. According to CBP officials, the ASTs are mobile autonomous surveillance towers with technologies that make use of artificial intelligence to better detect and identify items of interest. The information gathered from the ASTs is integrated with CBP's other digital coordination tools to increase overall situational awareness.

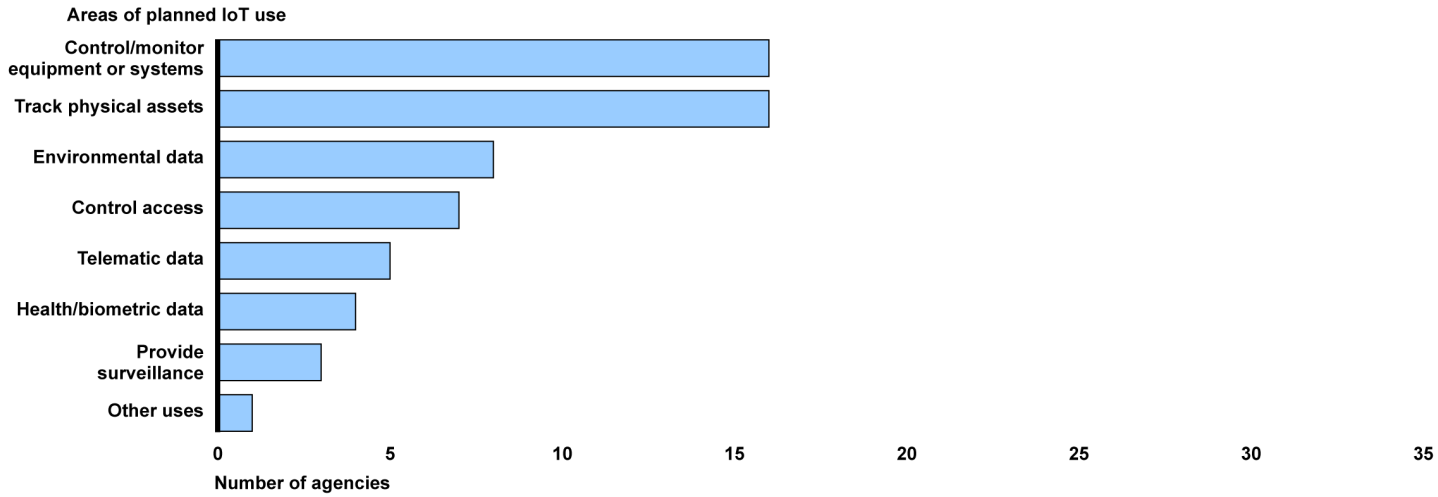
Many but Not All Federal Agencies Plan to Increase Use

According to the survey responses, federal agencies are planning to increase use of IoT. Many of the agencies (25 of 56) currently using IoT technologies indicated that they planned to expand IoT technology use in the next 5 years. For example, while EPA reported that it currently uses IoT technologies to collect environmental data, it also reported planning to

[21]The external braking system is a parachute-like structure intended to slow the test rocket's re-entry.

use IoT technologies to, among other things, track physical assets and control access to facilities. Furthermore, many agencies not currently using IoT technologies (21 of 34) reported that they plan to do so in the next 5 years. These agencies most frequently reported planning to use IoT technologies to track physical assets or to control and monitor equipment (see fig. 4).

Figure 4: Areas of Planned Internet of Things (IoT) Use by Federal Agencies Not Currently Using IoT Technologies



Source: GAO survey of federal agencies and sub-components. | GAO-20-577

Note: Twenty-one of the 34 federal agencies that said they are not currently using IoT reported on plans to use IoT technologies in one or more of these areas, while some of these agencies reported plans to use IoT technologies in more than one of these areas.

Notwithstanding the current and planned use of IoT technologies by federal agencies, 13 agencies reported that they were not currently using nor planning to use IoT technologies in the next 5 years. Federal agencies cited different reasons for not using IoT technologies: for example, one agency reported not seeing the return on investment, while another indicated the implementation burdens were difficult. Officials from NASA's Langley Research Center indicated there are likely many IoT technologies NASA could benefit from using, but the implementation process for these devices is too burdensome. In discussing this with NASA officials, they stated that connecting any device to their network can be challenging because NASA must research how these devices operate, including how the devices communicate and if they communicate with systems outside of NASA. Additionally, the Health Resources and Services Administration, which functions primarily to provide grants to

improve access to health care, responded that it does not have a business case for using IoT technologies.[22]

Many Agencies Acquire Commercial IoT Technologies

Both the agencies we surveyed and the case study agencies reported acquiring and using commercial IoT technologies. Most agencies reporting that they currently use IoT technologies (50 of 54), reported acquiring and using readily-available commercial IoT technologies. Similarly, all case study agencies also reported acquiring and using commercial IoT technologies and identified either timeliness, cost, or resource constraints as reasons they acquire and use such technologies, rather than developing their own. For example, officials at EPA told us that commercial companies can develop more advanced technologies faster than the agencies. The officials added that, while federal agencies have disparate missions, commercial companies' focus on researching and developing technologies, such as sensors. In addition, CBP officials told us that such technologies are often less expensive than developing the agency's own technologies. For instance, CBP officials told us that the commercial IoT products they use (e.g., devices to monitor vehicles at border entry points, among others,) are developed faster and at lower cost than if CBP had developed them internally.

While agencies may prefer to acquire and use commercially available IoT devices, DHS recently reported that commercially acquired IoT technologies may have inherent security vulnerabilities. For example, these commercially available devices may come with basic passwords that cannot be changed, or they may be susceptible to cyberattacks.[23] Some of these challenges are described later in this report.

Conversely, some agencies (17 of 73) reported that they are developing their own IoT technologies.[24] For example, CBP and NASA indicated they develop their own IoT technologies that are for specialized purposes and are therefore not available through commercial suppliers. For example, CBP officials told us they developed technologies to monitor trans-border tunnel threats and border wall breaches because of the specialty purpose

[22]The Health Resources and Services Administration is an agency of the U.S. Department of Health and Human Services.

[23]U.S. Department of Homeland Security, *Internet of Things Security Acquisition Guidance,* (Washington, D.C.: February, 2020).

[24]Not all survey respondents addressed this question, which asked if agencies develop their own IoT technologies. Thus the total number of responses to this question (73) are fewer than the total responses received for the survey (90).

of the technologies. Similarly, NASA officials told us they also developed some technologies internally because the nature and purpose of the technologies—those needed to operate in rockets during flight and communicate data—were unique. In developing these technologies, NASA officials also indicated they could then control the security and update protocol for the device, something that is not always possible with a commercially available device.

Federal Agencies Most Often Identified Increased Data Collection and Operational Efficiencies as Benefits and Cybersecurity and Interoperability as Challenges

Federal Agencies Identified Increased Data Collection and Operational Efficiencies, among Other Benefits Gained from IoT Technologies

Federal agencies responding to our survey identified four areas that benefited from IoT technologies:[25]

- **Data collection.** Many federal agencies (45 of 74) responding to our survey identified an improvement in data collection as a benefit of IoT technologies.[26] Two case study agencies noted that these technologies can provide real-time data to better inform and aid decision making. EPA officials reported using IoT sensors to provide real-time data during emergencies. For example, during a factory fire in New Jersey, EPA deployed sensors to monitor chlorine gas being

[25]The survey asked specifically how IoT technologies increased or decreased the following areas: operational costs, operational efficiency, operational productivity, energy consumption, data collection, programs and services automation, network security, and physical security. We also asked about what other effects IoT has on the respondents' agencies.

[26]Not all survey respondents addressed this question, which asked about the benefits to IoT technologies through increases or decreases across several areas. Thus, the total number of responses to this question (74) varied based on the respondents answering the question and are fewer than the total responses received for the survey (90).

released. The deployment provided a real-time picture of how the gas was dispersing. According to EPA officials, this helped EPA and other emergency responders coordinate a proper response, including directing some civilians to shelter in place. In addition, as discussed above, NASA reported that it tested IoT technologies to support the development of new space flight technologies. The IoT sensors collected and transmitted acceleration, temperature, and pressure data to help evaluate the effectiveness of the technology.

- **Operational efficiency.** Many federal agencies (43 of 74) responding to our survey also identified improving the efficiency of operations as a benefit of IoT technologies by allowing agencies to accomplish more with the same resources. For example, NOAA deployed unmanned systems–including aircraft, watercraft, and sensors on buoys–in conjunction with manned aircraft and ships to increase operational efficiencies. This deployment resulted in additional oceanographic and atmospheric data that support NOAA's research and reporting. EPA officials told us that data transmitted by IoT sensors eliminate the need for employees to visit sites to collect data. Previously, when collecting environmental data, EPA staff traveled to locations to download data from monitoring equipment. Now, for example, EPA staff no longer have to physically collect data from the water monitors in the Charles River because the data are now transmitted electronically. In addition, SLSDC officials said the hands-free mooring technology at their two vessel locks improved the speed of transit through SLSDC's lock system by approximately 5 to 7 minutes for each lock.[27]
- **Operational productivity.** An increase in operational productivity was identified by many federal agencies (40 of 74) as another benefit to IoT technologies. Agencies using IoT technologies reported that increases in output and that they were able to accomplish things they were not able to accomplish without this technology. CBP officials told us that IoT has allowed for faster processing of vehicles at its ports-of-entry compared with before the technology existed. This efficiency includes quickly identifying potential threats and being able to take action. It also includes quickly identifying vehicles as non-threats and keeping them moving through the entry process. Similarly to CBP, NOAA officials told us that IoT technology helped them increase productivity by placing sensors and collecting data in areas that may

[27]According to SLSDC officials, all locks across the system capable of using the hands-free mooring system (13 of 15) have the technology. While SLSDC does not track metrics for the Canadian operated locks, its Canadian counterparts have noted experiencing similar time improvements.

be difficult or impossible for humans to access and monitor such as around active volcanos.

- **Automated program and services.** Many federal agencies (40 of 74) responding to the survey indicated IoT technologies have increased the automation of programs and services. IoT devices are performing certain processes or services, thereby freeing up resources that had previously been responsible for performing these processes or services. As previously discussed, NOAA's National Ocean Service officials reported that in water labs, IoT technologies are used to monitor the cycling of water into labs to ensure water is pumped into the labs during high tide when the water is cleanest. Prior to this technology, this cycling of water and monitoring of the tides was manual and required staff to be present.

Additionally, some agencies responding to our survey noted that implementing IoT technologies would decrease costs (21 of 74).[28] We have previously reported that IoT technologies can reduce costs across various industries by, for example, identifying bottlenecks or reducing inefficiencies.[29] Similarly, a 2016 report found, "the primary motivation for federal agencies to use IoT is to be more efficient and reduce costs."[30] The report identified cost savings from programs that automate manual data-collection processes and increasing efficiencies in government vehicles and other benefits also identified in our survey responses. NOAA officials told us that in certain areas, deploying wireless IoT sensors is cost beneficial compared with deploying wired sensors. In 2015, EPA reported on the potential cost-savings based on a watershed demonstration project designed to collect and organize data from multiple sources into a single platform.[31] EPA found that full adoption of this IoT technology could result in approximately $6.3 million saved annually.

[28]A similar number of federal agencies (18 of 74) reported that IoT technologies would increase costs.

[29]GAO-17-75

[30]Castro, New, and McQuinn, *How Is the Federal Government Using the Internet of Things?*

[31]EPA, *E-enterprise For The Environment Return on Investment (ROI) Analysis Results* (July 2015).

Agencies Identified Cybersecurity and Interoperability with Legacy Systems as the Most Significant Challenges to Current and Future Use of IoT Technologies

Agencies responding to our survey reported that cybersecurity issues present the most significant challenge, and one case study agency has stopped IoT use and another decided not to adopt it for this reason. In our survey of federal agencies, cybersecurity was the most frequently cited challenge (43 of 74).[32] According to NIST, cybersecurity of IoT devices and the network they access presents a significant issue to the adoption of these technologies.[33] Case study agencies we spoke with identified specific cybersecurity challenges:

- According to officials at DHS's Transportation Security Administration (TSA), TSA cancelled plans to connect its airport security equipment as a result of new requirements put in place following a breach of federal employee information maintained by the Office of Personnel Management (OPM). In 2010, TSA began to connect its airport security equipment to its broader network of traveler data. The goal was to allow analysis of traveler data and sensor data from the security systems. According to officials, TSA stepped back from this program and removed all equipment from the network following OPM's breach because the security equipment and systems TSA was using could not meet the new cybersecurity requirements put in place in response to the breach.[34]
- As a result of developing an IoT lab, NASA identified a series of challenges to IoT and reported that cybersecurity was the most significant of these challenges.[35] In the IoT lab environment, NASA monitored IoT device activity to understand how, when, and with whom the devices and components were communicating and sharing data. According to NASA officials, they analyzed 50 devices and allowed NASA staff to bring in IoT devices, register the devices, and run a report to evaluate how the devices operated, communicated, and the amount of bandwidth. NASA determined, in part, that most

[32]The levels of challenge survey that respondents had to choose from were "very challenging", "somewhat challenging", "slightly challenging", "not at all challenging", "do not know", and "not applicable". For the purpose of ranking challenges, we summed the number of responses for "very challenging" and "somewhat challenging".

[33]NIST, NISTIR 8200 - *Interagency Report on the Status of International Cybersecurity Standardization for the Internet of Things (IoT),* (Gaithersburg, MD: November, 2018).

[34]According to agency officials, TSA mandated that acquisition of new security equipment must meet nine cybersecurity requirements before the equipment could be connected to the TSA network. For legacy devices, an agreed upon solution is still being investigated.

[35]NASA, *IoT Phase III White Paper (2018)*.

IoT devices could not be trusted on NASA networks and cybersecurity was the biggest concern.[36]

While agencies identified cybersecurity as a challenge, two of our case study agencies told us they are taking steps to address this challenge. These agencies indicated they were either operating or testing IoT technologies on segregated networks to mitigate the cybersecurity challenges. According to EPA officials, they capture data in a cloud environment, external to EPA's network, before introducing the data to the EPA network. Also, as part of its IoT lab, NASA's Johnson Space Center created a separate network to handle the testing of IoT devices. NASA took this step to secure its network and allow testing of these devices in a way that does not compromise the network.

Interoperability with legacy systems was the second most frequently cited challenge (30 of 74) by agencies.[37] As new IoT technologies develop, these technologies' ability or inability to work with existing technologies presents a challenge. If these systems are not interoperable, the benefits of IoT technologies can be limited.[38] According to NASA's Johnson Space Center officials, NASA has a number of legacy systems used to operate and launch space vehicles. These systems pre-date IoT technologies and were not designed to address risks inherent to IoT technologies. According to NASA officials, they segregated the IoT devices from the legacy systems because systems segregation allows the agency to control how the legacy systems interact with the IoT devices. However, NASA officials said that systems segregation eliminates some of the benefits that can be achieved with IoT technologies because the IoT data have to be imported into the legacy systems. NASA officials said they would like to take advantage of new technologies and are looking for ways to further address the interoperability issue.

[36]As priorities for NASA changed, the work in the IoT lab was concluded. Recommendations and lessons learned from the IoT lab at Johnson Space Center were captured in three working group white papers: *Internet of Things White Paper* (2015); *Internet of Things White Paper Phase II* (2017); and *IoT Phase III White Paper (2018)*.

[37]Even though this factor was identified as one of the top challenges, 20 agencies reported interoperability with legacy systems as slightly or not at all challenging.

[38]McKinsey Global Institute, *The Internet of Things: Mapping the Value Beyond the Hype* (2015)

There were other issues with IoT technologies identified in our survey that some federal agencies identified as being a challenge, although a similar number of agencies did not.

- **Knowledgeable personnel.** In response to the survey, about the same number of agencies identified knowledgeable personnel who know how to operate the devices or effectively use the data created by IoT devices as a challenge (29 of 74) as those reporting it was not a challenge (30 of 74). For example, the SLSDC identified a lack of trained personnel as a challenge to implementing the new automated hands-free mooring system for ships. According to SLSDC officials, some employees did not have the technical expertise to operate the new system. They addressed this challenge by providing training on the new system, and for those employees unable to learn the system, SLSDC shifted them to other operations and maintenance roles.
- **Privacy concerns.** Twenty-seven of 74 agencies responding to our survey identified ensuring the privacy of personally identifiable information as being a challenge, while 30 identified it as it not being a challenge.[39] This risk does not exist for all IoT devices because not all IoT devices process personally identifiable information. For example, EPA officials expressed that they generally did not have a concern with privacy because they process environmental data. However, TSA officials indicated that privacy was a significant concern in the development of its IoT systems because the agency was processing passenger information. In part, because TSA could not ensure the privacy of this data, and the security of the systems using this data, TSA removed security equipment processing passenger information from the network. According to agency officials, TSA found a solution and mitigated the risk, allowing TSA to begin reconnecting this security equipment in 2017.

[39]Personally identifiable information is information that can be used to locate or identify an individual, such as names, aliases, Social Security numbers, biometric records, and other personal information that is linked or linkable to an individual.

While Most Agencies Reported Using General Information Technology Policies, a Few Reported Using IoT-Specific Guidance

Most Agencies Use Their General Information Technology Policies to Use and Acquire IoT Technologies

Most agencies responding to our survey (54 of 72) reported using IT policies developed by their agency to manage IoT technologies.[40] These IT policies typically define responsibilities and requirements for the use and acquisition of IT. For example, EPA IT policies provide direction for managing information systems, defining oversight responsibilities, and establishing security requirements, among other practices.[41] According to EPA officials, these policies apply to any IoT technologies that are part of their network, but not to those that are external to the EPA network.[42] Similarly to EPA, NASA officials reported they have policies that apply to the management and security of IT that also apply to IoT technologies.[43] According to these officials, NASA's IT policies generally define the requirements and responsibilities and how to secure its systems and devices. Additionally, NOAA officials told us that the agency follows Commerce IT requirements, some of which are set forth in federal regulation. For example, the Commerce Acquisition Regulation directs the use of an acquisition checklist for all IT purchases that exceed a set

[40]Not all survey respondents addressed this question, thus the total responses to this question (72) are fewer than the total responses received for the survey (90).

[41]See, e.g., EPA, *Information Directive Policy: Information Security Policy*, Directive No: CIO 2150.5 (August 2019). According to EPA staff, EPA has numerous IT policies and directives that address all aspects of IT, and these apply to IoT technologies.

[42]According to EPA officials, the agency sometimes collects data from non-EPA sources not connected to its network. EPA's IT policies do not apply to these devices or the data that these devices collect.

[43]See, e.g., NASA, *NASA Policy Directive: Managing Information Technology*, NPD 2800.1E (Dec. 9, 2019); NASA, *NASA Procedural Requirements: Security of Information Technology,* NPR 2810.1B (May 16, 2006).

amount.[44] According to NOAA officials, the checklist ensures security and the supply chain's risk management requirements are built into the IT acquisition process.

Some agencies we spoke with reported their current IT policies were sufficient to address the current challenges and risks associated with IoT technologies, including cybersecurity. For example, DHS officials said that current IT policies are sufficiently broad to account for the effect of IoT technologies. Similarly, NASA officials told us that current IT policies were sufficient to address the cybersecurity challenges IoT presents. Furthermore, they regularly review these policies, and, if additional clarification or guidance is needed, it can be done as part of this regular process.

Many agencies (37 of 71) also reported using broad, governmentwide policies, such as OMB's *Circular A-130* to guide their agencies' use of IoT. OMB *Circular A-130* establishes general policy for, among other things, the governance, acquisition, and management of Federal IT resources and supporting infrastructure.[45] The Circular also requires agencies to consult NIST standards and guidelines when it comes to information security. According to OMB officials, OMB has not developed IoT policies, and it therefore expects agencies to apply the directives from OMB *Circular A-130* to IoT, as it would for any other IT. OMB officials told us the agency does not usually make policy for specific IT components, such as IoT, but relies on broader IT policies. However, they told us that if in conjunction with NIST, it was determined that an IoT policy was needed, OMB would work with NIST and others to develop such a policy.

Few Agencies Reported Using IoT-specific Guidance

Three agencies we surveyed mentioned using IoT-specific government-wide guidance.[46] Examples of this government-wide guidance include a series of NIST reports outlining cybersecurity guidance and proposed

[44]48 C.F.R. §1339.107-70. This federal regulation requires that for all service acquisitions over the micro-purchase threshold, contracting professionals shall coordinate with the designated Contracting Officer Representative (COR) to complete the Information Security in Acquisition Checklist.

[45]Managing Information as a Strategic Resource, 81 Fed. Reg. 49689 (July 28, 2016)

[46]Not all survey respondents addressed this question, which asked if agencies use IoT-specific government-wide guidance, thus the total number of responses to this question (57) is fewer than the total responses received for the survey (90).

standards for IoT technologies.[47] In 2018, NIST published an interagency report that addressed cybersecurity standards for IoT technologies.[48] The purpose of the report was to facilitate communication and understanding among federal agencies about IoT cybersecurity challenges and solutions. In 2019, NIST issued a report that provided guidance to help agencies understand and manage specific cybersecurity and privacy risks associated with IoT devices throughout the devices' lifecycles.[49]

In addition to the guidance agencies identified in the survey, DHS issued two reports providing guidance on security for IoT. The first, issued in 2016, developed strategic principles for securing IoT technologies, including suggested practices to secure network-connected devices.[50] These principles were designed to be used throughout the IoT supply chain, by IoT device developers, manufacturers, and consumers (including the federal government). According to DHS, widespread adoption of these suggested principles could improve an agency's IoT security. Some of the practices DHS identified that incorporate these principles include, among other things, developing devices that do not come with standard or easy-to-crack passwords, coordinating software updates among IoT vendors, and authenticating all devices connected to the network. The second report, issued in 2020, provided guidance for security issues agencies should consider when acquiring IoT technologies.[51] The guidance recommended improvements to the effectiveness of supply-chain, vendor, and technology evaluations prior to the purchase of IoT devices and services.

While fewer agencies reported having or using IoT-specific policies and guidance (19 of 69) than reported using general internal IoT policies and

[47]NIST's Cybersecurity for the Internet of Things program supports 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. By collaborating with stakeholders across government, industry, international bodies, and academia, the program aims to cultivate trust and foster an environment that enables innovation on a global scale.

[48]NIST, NISTIR 8200 - *Interagency Report on the Status of International Cybersecurity Standardization for the Internet of Things (IoT)* (Gaithersburg, MD: November 2018).

[49]NIST, *Considerations for Managing Internet of Things Cybersecurity and Privacy Risks,* NISTIR 8228 (Gaithersburg, MD: June 2019).

[50]DHS, *Strategic Principles for Securing the Internet of Things (IoT)* (Washington, D.C.: Nov. 15, 2016).

[51]DHS, *Internet of Things Security Acquisition Guidance* (Washington, D.C.: Feb. 11, 2020).

guidance, officials at three of the four case study agencies mentioned that there could be an opportunity for such policies and guidance at their agencies. At NASA, as part of work supporting the IoT lab, NASA officials identified the need for an IoT policy that was designed to address any device that connects to its network. A proposed policy was developed, but, according to NASA officials, the concerns and issues addressed by the proposed IoT-specific guidance were incorporated into existing agency IT guidance. EPA officials from the Office of Water indicated there was no specific IoT policy or guidance but thought it may be worth considering, given the growth in IoT technologies. However, EPA officials stated that if any IoT-specific policies were developed, they would have to be defined within the program using them, and align with EPA's IT policies. NOAA officials said specific IoT policies could be helpful in promoting increased use of IoT technologies for scientific research purposes.

However, there are diverse views on whether there is a need for government-wide policies and guidance specific to IoT. As reported above, some agency officials told us that existing IT policies and guidance were adequate for managing and acquiring IoT technologies and addressing the current challenges and associated risks, including cybersecurity. As previously discussed, OMB officials said they would work with NIST and others to develop IoT specific policies if it were determined such policies were needed. According to NIST officials, current government-wide IT policies include IoT technologies, and therefore there is no need for additional IoT-specific policies at this time, but as IoT use increases, NIST will continue to monitor whether there is a need for change.

Agency Comments

We provided a draft of this report to Commerce, DOD, DHS, DOT, EPA, NASA, and OMB. In response, Commerce, DHS, and OMB provided technical comments, which we incorporated as appropriate. The other agencies reviewed the report but did not provide any comments.

As agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the report date. We are sending copies of this report to the Secretaries of Commerce, Defense, Homeland Security, and Transportation, the Administrators of NASA and EPA, the Director of OMB, and appropriate congressional committees. In addition, the report will be available at no charge on the GAO website at http://www.gao.gov.

If you or members of your staff have any questions about this report, please contact me at (202) 512-2834 or vonaha@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Major contributors to this report are listed in appendix IV.

Andrew Von Ah
Director, Physical Infrastructure Issues

Appendix I: Survey of Federal Agencies on Use and Acquisition of Internet of Things Technologies

To obtain information about federal agencies' use of Internet of Things (IoT) technologies, in December 2019, we surveyed 115 federal agencies' Chief Information Officers (CIO) or senior information technology managers at selected federal agencies and sub-components. We asked a series of closed- and open-ended questions about: (1) the extent to which each agency is using IoT technologies; (2) the purposes for which IoT technologies are used; (3) the policies and guidance that inform the use and acquisition of IoT technologies; and (4) the benefits and challenges associated with acquiring and using IoT technologies, among other things. The questions we asked and the aggregate results of the responses to the closed-ended questions are shown below. We do not provide results for the open-ended questions, but some of the open-ended responses were used as examples throughout the report. We received 90 completed survey responses—a response rate of 78 percent.[1]

1. Please provide your contact information.
2. Does your agency use, or plan to use in the next five years, IoT technologies to perform any of the following tasks?

2a. Collect environmental data (e.g., atmospheric, geologic, oceanographic) n=90		
Response	**Number of Responses**	**Percent**
Yes, currently using	23	25.56
Yes, planning to use	14	15.56
No, neither using nor planning to use	45	50.00
Don't know	8	8.89

[1]This represents the number of surveys we received back in relation to the number of surveys we sent out. However, not all surveys had a response to each question. The number of total responses for each question is indicated at the end of the respective question and varies. The percentages listed next to each response reflects the percentage of all responses for that question.

2b. Collect health/biometric data (e.g., heart rate, blood glucose, fingerprint, etc.) n=90

Response	Number of Responses	Percent
Yes, currently using	17	18.89
Yes, planning to use	10	11.11
No, neither using nor planning to use	55	61.11
Don't know	8	8.89

2c. Collect telematic data (e.g., speed, acceleration, deceleration, gravitational force, etc.) n=89

Response	Number of Responses	Percent
Yes, currently using	15	16.85
Yes, planning to use	13	14.61
No, neither using nor planning to use	50	56.18
Don't know	11	12.36

2d. Control/monitor equipment or systems (e.g., turn equipment on or off, regulate systems, etc.) n=90

Response	Number of Responses	Percent
Yes, currently using	42	46.67
Yes, planning to use	21	23.33
No, neither using nor planning to use	19	21.11
Don't know	8	8.89

2e. Track physical assets (i.e., fleet vehicles, personal property, equipment, etc.) n=89

Response	Number of Responses	Percent
Yes, currently using	28	31.46
Yes, planning to use	26	29.21
No, neither using nor planning to use	22	24. 72
Don't know	13	14.61

2f. Control access (e.g., fingerprint/retina scanners to unlock a device, provide access to a building/room, etc.) n=89

Response	Number of Responses	Percent
Yes, currently using	39	43.82
Yes, planning to use	12	14.48
No, neither using nor planning to use	29	32.58
Don't know	9	10.11

2g. Provide human surveillance (e.g., GPS tracking, facial recognition to surveil people in a crowd, etc.) n=89		
Response	**Number of Responses**	**Percent**
Yes, currently using	15	16.85
Yes, planning to use	9	10.11
No, neither using nor planning to use	53	59.55
Don't know	13	13.48

2h. Other use n=85		
Response	**Number of Responses**	**Percent**
Yes, currently using	8	9.41
Yes, planning to use	5	5.88
No, neither using nor planning to use	26	30.59
Don't know	46	54.12

2i. What other use? (written responses not included)

3. Are there IoT technologies you think could help your agency, but which your agency is neither using nor planning to use in the next five years? n=89

Response	Number of Responses	Percent
Yes, currently using	20	22.47
Yes, planning to use	31	34.83
Don't know	38	42.70

4. How long has your agency been using IoT technologies? n=89

Response	Number of Responses	Percent
Less than 3 years	18	20.22
3 years to less than 5 years	14	15.73
5 years or more	32	35.96
My agency does not currently use IoT technologies	25	28.09

5. Has your agency developed its own IoT technologies? n=73

Response	Number of Responses	Percent
Yes	17	23.29
No	50	68.49
Don't know	6	8.22

5a. Please describe the IoT technologies your agency has developed. (Written responses not included)

6. Has your agency used commercial off-the-shelf (COTS) IoT technologies? n=73

Response	Number of Responses	Percent
Yes	59	80.82
No	10	13.70
Don't know	4	5.48

7. Is there one person at your agency that has overall responsibility for the use of IoT technologies? n=73

Response	Number of Responses	Percent
Yes	14	19.18
No	55	75.34
Don't know	4	5.48

7a. What is the person's job title? (Written responses not included)

8. What is/are the job title(s) of the person(s) at your agency that manage(s) the day-to-day use of IoT technologies? (Written responses not included)

9. Is there one person at your agency that has overall responsibility for the acquisition of IoT technologies? n=74

Response	Number of Responses	Percent
Yes	22	29.73
No	46	62.16
Don't know	6	8.11

9a. What is the person's job title? (Written responses not included)

10. Which of the following, if any, guides your agency's use of IoT technologies?

10a. Internal IT guidance n=72		
Response	**Number of Responses**	**Percent**
Yes	54	75.00
No	15	20.83
Don't know	3	4.17

10b. IoT-specific internal policies n=68		
Response	**Number of Responses**	**Percent**
Yes	14	20.59
No	46	67.65
Don't know	8	11.76

10c. IoT-specific internal guidance n=69		
Response	**Number of Responses**	**Percent**
Yes	17	24.64
No	42	60.87
Don't know	10	14.49

10d. Other n=57		
Response	**Number of Responses**	**Percent**
Yes	21	36.84
No	13	22.81
Don't know	23	40.35

10e. Please specify what else guides your agency's use of IoT technologies. (Written responses not included)

11. Which of the following, if any, guides your agency's acquisition of IoT technologies?

11a. Internal IT guidance n=73		
Response	**Number of Responses**	**Percent**
Yes	56	76.71
No	14	19.18
Don't know	3	4.11

11b. IoT-specific internal policies n=67

Response	Number of Responses	Percent
Yes	14	20.90
No	44	65.67
Don't know	9	13.43

11c. IoT-specific internal guidance n=67

Response	Number of Responses	Percent
Yes	16	23.88
No	41	61.19
Don't know	10	14.93

11d. Other n=59

Response	Number of Responses	Percent
Yes	21	35.59
No	18	30.51
Don't know	20	33.90

11e. Please specify what else guides your agency's acquisition of IoT technologies? (Written responses not included)

12. Is your agency's use of IoT technologies guided by government-wide policy(s) or guidance? (e.g. OMB) n=71

Response	Number of Responses	Percent
Yes	37	52.11
No	34	47.89

12a. Please provide the name of the policy. (Written responses not included)

13. At your agency, how much does the use of IoT technologies decrease or increase the following items?

13a. Operational costs n=74

Response	Number of Responses	Percent
Greatly decrease	6	8.11
Slightly decrease	15	28.38
No change	6	8.11
Slightly increase	12	16.22
Greatly increase	6	8.11
Don’t know	18	24.32
Not applicable	11	14.86

13b. Operational efficiency n=74

Response	Number of Responses	Percent
Greatly decrease	2	2.710
Slightly decrease	1	1.35
No change	2	2.70
Slightly increase	19	25.68
Greatly increase	24	33.43
Don’t know	16	21.62
Not applicable	10	13.51

13c. Operational productivity n=74

Response	Number of Responses	Percent
Greatly decrease	2	2.70
Slightly decrease	-	-
No change	4	5.41
Slightly increase	18	24.32
Greatly increase	22	29.73
Don’t know	18	24.32
Not applicable	10	13.51

13d. Energy Consumption n=75		
Response	**Number of Responses**	**Percent**
Greatly decrease	2	2.70
Slightly decrease	13	17.57
No change	16	21.62
Slightly increase	8	10.81
Greatly increase	3	4.05
Don’t know	20	27.03
Not applicable	12	16.22

13e. Data collection n=74		
Response	**Number of Responses**	**Percent**
Greatly decrease	2	2.70
Slightly decrease	1	1.35
No change	3	4.05
Slightly increase	23	31.08
Greatly increase	22	29.73
Don’t know	15	20.27
Not applicable	8	10.81

13f. Automate programs or services n=74		
Response	**Number of Responses**	**Percent**
Greatly decrease	2	2.70
Slightly decrease	2	2.70
No change	4	5.41
Slightly increase	20	27.03
Greatly increase	20	27.03
Don’t know	15	20.27
Not applicable	11	14.86

13g. Security of the network n=73		
Response	**Number of Responses**	**Percent**
Greatly decrease	4	5.48
Slightly decrease	13	17.81
No change	12	16.44
Slightly increase	11	15.07
Greatly increase	8	10.96
Don't know	16	21.92
Not applicable	9	12.33

13h. Physical security n=72		
Response	**Number of Responses**	**Percent**
Greatly decrease	1	1.39
Slightly decrease	5	6.94
No change	10	13.89
Slightly increase	21	29.17
Greatly increase	11	15.28
Don't know	15	20.83
Not applicable	9	12.50

14. What other effects, if any, does IoT usage have on your agency? (Written responses not included)

15. How challenging, if at all, have the following items been in the deployment of IoT technologies?

15a. Procurement n=72		
Response	**Number of Responses**	**Percent**
Very challenging	8	11.11
Somewhat challenging	14	19.44
Slightly challenging	15	20.83
Not at all challenging	14	19.44
Don't know	12	16.67
Not applicable	9	12.50

15b. Funding n=74

Response	Number of Responses	Percent
Very challenging	13	17.57
Somewhat challenging	16	21.62
Slightly challenging	14	18.92
Not at all challenging	11	14.86
Don't know	10	13.51
Not applicable	10	13.51

15c. Knowledgeable personnel n=74

Response	Number of Responses	Percent
Very challenging	9	12.16
Somewhat challenging	20	27.03
Slightly challenging	18	24.32
Not at all challenging	12	16.22
Don't know	7	9.46
Not applicable	8	10.81

15d. Interoperability with other IoT devices n=74

Response	Number of Responses	Percent
Very challenging	8	10.81
Somewhat challenging	12	16.22
Slightly challenging	22	29.73
Not at all challenging	8	10.81
Don't know	11	14.86
Not applicable	13	17.57

15e. Interoperability with legacy systems n=74

Response	Number of Responses	Percent
Very challenging	18	24.32
Somewhat challenging	12	16.22
Slightly challenging	15	20.27
Not at all challenging	5	6.76
Don't know	7	9.46
Not applicable	17	22.97

15f. Privacy concerns n=74

Response	Number of Responses	Percent
Very challenging	14	18.92
Somewhat challenging	13	17.57
Slightly challenging	22	29.73
Not at all challenging	8	10.81
Don't know	7	9.46
Not applicable	10	13.51

15g. Cybersecurity concerns n=74

Response	Number of Responses	Percent
Very challenging	27	36.49
Somewhat challenging	16	21.62
Slightly challenging	11	14.86
Not at all challenging	5	6.76
Don't know	5	6.76
Not applicable	10	13.51

15h. Spectrum availability n=74

Response	Number of Responses	Percent
Very challenging	6	8.11
Somewhat challenging	10	13.51
Slightly challenging	11	14.86
Not at all challenging	10	13.51
Don't know	20	27.03
Not applicable	17	22.97

15i. Other item n=61

Response	Number of Responses	Percent
Very challenging	3	4.92
Somewhat challenging	1	1.64
Slightly challenging	0	0.00
Not at all challenging	4	6.56
Don't know	19	31.15
Not applicable	34	55.74

15j. What is the other challenge? (Written responses not provided)

16. Please describe the two most significant challenges identified in Question 17. (Written responses not provided)

17. What measures, if any, has your agency taken to address these two most significant challenges? (Written responses not provided)

Appendix II: List of Federal Agencies and Sub-Components That Received the Survey

The table provides all federal agencies and sub-components surveyed (see table 1). The federal agencies in bold are members of the Federal Chief Information Officers Council; however, only the numbered agencies and sub-components received the survey. See appendix III for more information on how we selected the federal agencies and sub-components we surveyed.

Table 1: List of Agencies and Sub-Components Surveyed

Department of Agriculture	
1. Agricultural Marketing Service	8. Foreign Agricultural Service
2. Agricultural Research Service	9. Forest Service
3. Animal and Plant Health Inspection Service	10. National Agricultural Statistics Service
4. Economic Research Service	11. National Institute of Food and Agriculture
5. Farm Service Agency	12. Natural Resources Conservation Service
6. Food and Nutrition Service	13. Risk Management Agency
7. Food Safety and Inspection Service	14. Rural Development
Department of Defense	
15. Army Corps of Engineers	18. Department of the Navy
16. Department of the Air Force	19. United States Marine Corps
17. **Department of the Army**	
Department of Commerce	
20. Bureau of Economic Analysis	26. National Institute of Standards and Technology
21. Bureau of Industry and Security	27. National Oceanic and Atmospheric Administration
22. Census Bureau	28. National Technical Information Service
23. Economic Development Administration	29. National Telecommunications and Information Administration
24. International Trade Administration	
25. Minority Business Development Agency	
30. Department of Education	
Department of Energy	
31. Energy Information Administration	32. National Nuclear Security Administration
Department of Health and Human Services	
33. Administration for Children and Families	39. Centers for Medicare and Medicaid Services
34. Administration for Community Living	40. Food and Drug Administration
35. Agency for Healthcare Research and Quality	41. Health Resources and Services Administration
36. Agency for Toxic Substances and Disease Registry	42. Indian Health Service
37. Center for Faith-Based and Neighborhood Partnerships	43. National Institutes of Health
38. Centers for Disease Control and Prevention	44. Substance Abuse and Mental Health Services Administration
Department of Homeland Security	

45. Customs and Border Protection	50. Transportation Security Administration
46. Cybersecurity and Infrastructure Security Agency	51. United States Citizenship and Immigration Services
47. Federal Emergency Management Agency	52. United States Coast Guard
48. Federal Law Enforcement Training Centers	53. United States Secret Service
49. Immigration and Customs Enforcement	
54. Department of Housing and Urban Development	
Department of the Interior	
55. Bureau of Indian Affairs	60. Fish and Wildlife Service
56. Bureau of Land Management	61. National Park Service
57. Bureau of Ocean Energy Management	62. Office of Surface Mining Reclamation and Enforcement
58. Bureau of Reclamation	63. United States Geological Survey
59. Bureau of Safety and Environmental Enforcement	
Department of Justice	
64. Bureau of Alcohol, Tobacco, Firearms and Explosives	67. Drug Enforcement Administration
65. Bureau of Prisons	68. Federal Bureau of Investigations
66. Community Relations Service	69. United States Marshals Service
Department of Labor	
70. Bureau of Labor Statistics	74. Occupational Safety and Health Administration
71. Employee Benefits Security Administration	75. Pension Benefit Guaranty Corporation
72. Employment and Training Administration	76. Veterans' Employment and Training Service
73. Mine Safety and Health Administration	
Department of State	
77. Bureau of Intelligence and Research	78. Bureau of Legislative Affairs
Department of Transportation	
79. Federal Aviation Administration	84. Maritime Administration
80. Federal Highway Administration	85. National Highway Traffic Safety Administration
81. Federal Motor Carrier Safety Administration	86. Pipeline and Hazardous Materials Safety Administration
82. Federal Railroad Administration	87. Saint Lawrence Seaway Development Corporation
83. Federal Transit Administration	
Department of Treasury	
88. Alcohol and Tobacco Tax and Trade Bureau	92. Internal Revenue Service
89. Bureau of Engraving and Printing	93. Comptroller of the Currency
90. Bureau of the Fiscal Service	94. United States Mint
91. Financial Crimes Enforcement Network	
95. Department of Veterans Affairs	
96. Environmental Protection Agency	
General Services Administration	
97. Federal Acquisition Service	98. Public Buildings Service
National Aeronautics and Space Administration	

99. Ames Research Center	104. Kennedy Space Center
100. Armstrong Flight Research Center	105. Langley Research Center
101. Glenn Research Center	106. Marshall Space Flight Center
102. Goddard Space Flight Center	107. Stennis Space Center
103. Johnson Space Center	
108. National Archives and Records Administration	
109. National Science Foundation	
110. Nuclear Regulatory Commission	
111. Office of Management and Budget	
112. Office of Personnel Management	
113. Small Business Administration	
114. Social Security Administration	
115. U.S. Agency for International Development	

Source: GAO | GAO-20-577

Appendix III: Objectives, Scope and Methodology

This report addresses (1) the Internet of Things (IoT) technologies federal agencies are using, (2) the benefits and challenges agencies associated with using IoT technologies, and (3) the policies and guidance that agencies use to manage the use and acquisition of IoT technologies.

To meet these reporting objectives, we surveyed 115 federal agencies, conducted case studies of selected agencies that use IoT technologies, and reviewed documents relevant to federal IoT use and acquisition. We also reviewed laws related to IoT such as the Federal Information Technology Acquisition Reform Act and the Federal Information Security Modernization Act of 2014, and interviewed officials at the Office of Management and Budget (OMB), National Institute of Standards and Technology (NIST), and the National Telecommunications and Information Administration (NTIA). The information below describes how we conducted the survey and how we selected the case study agencies.

Survey of Federal Chief Information Officers

To describe the IoT technologies federal agencies are currently using, the benefits and challenges of these technologies, and the policies and guidance the agencies have to direct the use and acquisition of IoT technologies, we conducted a survey of Chief Information Officers (CIO) and senior information technology officials at federal agencies. In an effort to manage the scope of the survey, we focused on federal departments and agencies that comprise the CIO Council and selected sub-components of these departments and agencies.[1] We used the CIO Council as these agencies comprise the principal interagency forum to improve agency practices related to information technology (IT). Further, to identify a selected number of possible sub-components that could speak to IoT use, we selected sub-components classified as administration, agency, authority, bureau, center, corporation, institute, or service, and we excluded subordinate components classified as board, commission, directorate, division, or office or any other component name not mentioned above. For larger agencies, such as the Department of

[1]The Federal CIO Council consists of the CIOs of the following 28 agencies: Army Corps of Engineers, Department of Agriculture, Department of the Air Force, Department of the Army, Department of Defense, Department of Commerce, Department of Education, Department of Energy, Department of Health and Human Services, Department of Homeland Security, Department of Housing and Urban Development, Department of the Interior, Department of Justice, Department of Labor, Department of State, Department of Transportation, Department of the Treasury, Department of Veteran Affairs, Environmental Protection Agency, General Services Administration, National Aeronautics and Space Administration, National Archives and Records Administration, National Science Foundation, Nuclear Regulatory Commission, Office of Management and Budget, Office of Personnel Management, Small Business Administration, Social Security Administration, and the U.S. Agency for International Development.

Transportation, we used these criteria to select the sub-component organizations to participate in our survey. However, for the CIO Council's smaller member agencies such as the Small Business Administration, we surveyed the CIO of the top-level of the organization because these agencies do not have any subordinate components that meet the above criteria. Additionally, for the CIO Council's member agencies that have only one sub-component that met the above criteria, we also only surveyed the CIO at the top-level of the organization. We limited our universe to sub-components of the organization that oversee programs, and excluded geographic, regional, or site-specific sub-components, as well as, support components. We excluded 13 agencies that informed us that their IT functions were performed by another entity within their organization. By applying these selection criteria, we established a population of 115 agencies (see app. II for a full list of agencies and sub-components that received the survey). We contacted audit liaisons at each of the agencies to obtain or confirm the CIO's or senior IT executive's contact information, and to advise them on the survey timeframes, including when to expect the survey.

We conducted pre-tests with CIOs or senior IT executives at the Department of Agriculture, Department of Justice, and the General Services Administration, to check that (1) the questions were clear and unambiguous; (2) the terminology was used correctly; (3) the questionnaire did not place an undue burden on agency officials; (4) the information could feasibly be obtained; and (5) the survey was comprehensive and unbiased. We then modified the survey based on feedback received during the pretests. We conducted the web-based survey from December 16, 2019, to February 12, 2020, which included both email and phone follow-up with non-respondents. We received 90 survey responses, giving us a 78 percent response rate. However, not all surveys had a response to each question so the total number of responses for each question varies throughout the report. When discussing the survey results in this report, there are occasions we use the terms "some", "many", and "most". For the purposes of reporting these survey results, "some" refers to a quantity of one-third or less of a question's responses; "many" refers to refers to a quantity of responses between one-third and two-thirds; and "most" refers to quantities that are two-thirds or greater of a question's total responses.

Case Studies

To learn more about how agencies are using IoT technologies, the benefits and challenges they experience, and the policies and guidance they use, we selected four case study agencies from the Federal CIO Council to review based on three selection criteria: the agencies' fiscal

year 2020 budget for information technology, use case examples found in literature, and the mission of the agencies. In reviewing the CIO Council's member agency IT budgets, we selected three agencies with fiscal year 2020 IT budgets over $1 billion to provide the perspectives of larger agencies, and one agency with a fiscal year budget under $1 billion to provide the perspective of a smaller agency (using the IT budget as a proxy for agency size). We also narrowed the field of agencies to select as case studies based on various IoT uses identified through a literature review. We did this to provide assurance that the agencies we included had experience using IoT technologies in support of their missions. The last criterion was that the agencies selected reflect a variety of agency missions. Of the agencies we identified through first two criteria, we wanted at least one agency with a security mission and one with a science mission. We defined "security" agencies as those that focus on protecting and preventing physical attacks or cyberattacks against the United States and its people. We defined "science" agencies as those that support and guide advancements in science and technology for both the federal government and the private sector. We excluded the General Services Administration and the Department of Transportation from this list for consideration because of work GAO has previously done on IoT topics with each of these agencies.[2] We also excluded Department of Defense (DOD) from our selection because there is significant investment in this technology within DOD that could warrant its own study. However, each of these agencies were included in the survey conducted.

Based on these criteria, we selected the following CIO Council's member agencies to include as case studies:

- Department of Commerce (Commerce)
- Department of Homeland Security (DHS)
- Environmental Protection Agency (EPA)
- National Aeronautics and Space Administration (NASA)

Within each case study agency, we interviewed officials from the Office of the CIO at the department level. We also interviewed officials at selected sub-component agencies at each of the selected departments. At Commerce, we met with a staff member from the Office of the CIO, as well as the CIO or officials at the National Oceanic and Atmospheric Administration. We also met with relevant officials at the National Institute

[2]We reported on the GSA smart buildings program in GAO-18-200 and the DOT vehicle-to-vehicle and vehicle-to-infrastructure in GAO-14-13 and GAO-15-775, respectively.

of Standards and Technology. At DHS, we interviewed staff from the Office of the CIO or other officials from the Science and Technology Directorate, the Cybersecurity and Infrastructure Security Agency, Customs and Border Protection, and the Transportation Safety Administration. At EPA, we met with officials from the Office of the CIO and officials from the Office of Water, and the Office of Land and Emergency Management. At NASA, we met with representatives from the Office of the CIO, as well as, the Chief Technology Officer at Johnson Space Center, the CIO at Langley Research Center, and a researcher at Ames Research Center working on IoT issues. For each case study agency, we also reviewed relevant IT and other policies, as well as, relevant reports and other documents related to agencies' IoT use.

Appendix IV: GAO Contacts and Staff Acknowledgments

GAO Contacts

Andrew Von Ah at (202)512-2834 or vonah@gao.gov

Staff Acknowledgments

In addition to the contact names above individuals making contributions to this report included Derrick Collins (Assistant Director); Eric Hudson (Analyst-in-Charge); Oluwaseun Ajayi; Jennifer Beddor; Christa Burdick; Dave Dornisch; Kaelin Kuhn; Josh Ormond; Steve Rabinowitz; Amy Rosewarne; Kelly Rubin; Andrew Stavisky; and Janet Temko-Blinder.