United States Government Accountability Office

Report to Congressional Committees

July 2017

INTERNET OF THINGS

Enhanced Assessments and Guidance Are Needed to Address Security Risks in DOD

Accessible Version

GAO Highlights

Highlights of GAO-17-668, a report to congressional committees

July 2017

INTERNET OF THINGS

Enhanced Assessments and Guidance Are Needed to Address Security Risks in DOD

Why GAO Did This Study

Congress included provisions in reports associated with two separate statutes for GAO to assess the IoT-associated security challenges faced by DOD. This report (1) addresses the extent to which DOD has identified and assessed security risks related to IoT devices, (2) assesses the extent to which DOD has developed policies and guidance related to IoT devices, and (3) describes other actions DOD has taken to address security risks related to IoT devices.

GAO reviewed reports and interviewed DOD officials to identify risks and threats of IoT devices faced by DOD. GAO also interviewed DOD officials to identify risk assessments that may address IoT devices and examined their focus areas. GAO further reviewed current policies and guidance DOD uses for IoT devices and interviewed officials to identify any gaps in policies and guidance where security risks may not be addressed.

What GAO Recommends

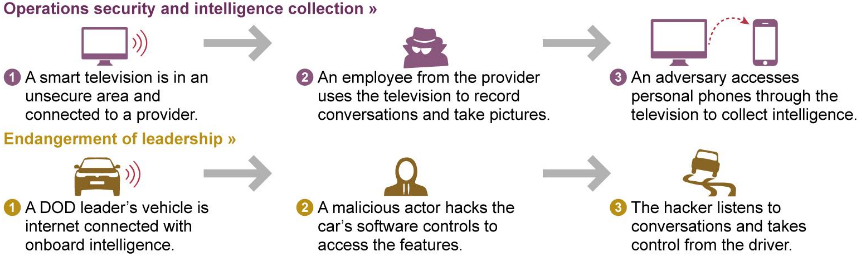
GAO recommends that DOD (1) conduct operations security surveys that could address IoT security risks or address operations security risks posed by IoT devices through other DOD risk assessments; and (2) review and assess its security policies and guidance affecting IoT devices and identify areas, if any, where new DOD policies may be needed or where guidance should be updated. DOD reviewed a draft of this report and concurs with GAO's recommendations.

View GAO-17-668. For more information, contact Joseph W. Kirschbaum at (202) 512-9971 or KirschbaumJ@gao.gov.

What GAO Found

The Internet of Things (IoT) is the set of Internet-capable devices, such as wearable fitness devices and smartphones, that interact with the physical environment and typically contain elements for sensing, communicating, processing, and actuating. Even as the IoT creates many benefits, it is important to acknowledge its emerging security implications. The Department of Defense (DOD) has identified numerous security risks with IoT devices and conducted some assessments that examined such security risks, such as infrastructure-related and intelligence assessments. Risks with IoT devices can generally be divided into risks with the devices themselves and risks with how they are used. For example, risks with the devices include limited encryption and a limited ability to patch or upgrade devices. Risks with how they are used—operational risks—include insider threats and unauthorized communication of information to third parties. DOD has developed IoT threat scenarios involving intelligence collection and the endangerment of senior DOD leadership—scenarios that incorporate IoT security risks (see figure). Although DOD has begun to examine security risks of IoT devices through its infrastructure-related and intelligence assessments, the department has not conducted required assessments related to the security of its operations.

Notional Internet of Things (IoT) Scenarios Identified by Department of Defense (DOD)


Operations security and intelligence collection »
1 A smart television is in an unsecure area and connected to a provider.
2 An employee from the provider uses the television to record conversations and take pictures.
3 An adversary accesses personal phones through the television to collect intelligence.
Endangerment of leadership »
1 A DOD leader's vehicle is internet connected with onboard intelligence.
2 A malicious actor hacks the car's software controls to access the features.
3 The hacker listens to conversations and takes control from the driver.

Source: GAO analysis of Department of Defense (DOD) information. | GAO-17-668

DOD has 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, GAO found that these policies and guidance do not clearly address some security risks relating to IoT devices. First, current DOD policies and guidance are insufficient for certain DOD-acquired IoT devices, such as smart televisions in unsecure areas, and IOT device applications. Secondly, DOD policies and guidance on cybersecurity, operations security, information security, and physical security do not address IoT devices. Lastly, DOD does not have a policy directing its components to implement existing security procedures on industrial control systems—including IoT devices. Updates to DOD policies and guidance would likely enhance the safeguarding and securing of DOD information from IoT devices.

This is an unclassified version of a sensitive report GAO issued in June 2017.

Contents

Tables

Figures

Abbreviations

DOD	Department of Defense
IoT	Internet of Things

U.S. GOVERNMENT ACCOUNTABILITY OFFICE

441 G St. N.W.
Washington, DC 20548

July 27, 2017

Congressional Committees

According to a Defense Science Board study, the Internet of Things (IoT) is the set of Internet Protocol-addressable devices that interact with the physical environment and typically contain elements for sensing, communicating, processing, and actuating.[1] With such capabilities—including personal smart devices acquired and used by Department of Defense (DOD) employees (e.g., wearable fitness devices), smart devices that DOD acquires (e.g., smartphones), and smart devices that DOD vendors may acquire and install on DOD installations (e.g., devices within industrial and utility control systems)—being given Internet access and thus becoming part of the IoT, DOD has stated that it is entering a rapidly deepening pool of vulnerability. The IoT has the potential to affect economies and societies throughout the world, from consumer products to industrial processes and public services.[2] Even as the IoT creates many benefits, it is important to acknowledge the many security implications that may arise. Although DOD has been using automated sensors and controls for more than a century and has been connecting them to computers for decades, the department is now in the midst of enormous technological change. While there have always been risks to DOD sensors and controls, their proprietary nature and isolation previously limited the possibility of attack, according to a DOD document about the IoT.[3]

According to the Director of National Intelligence, IoT devices are designed and fielded with minimal security requirements and testing, and an ever-increasing complexity of networks could lead to widespread vulnerabilities in civilian infrastructures and U.S. government

[1] Defense Science Board, *Summer Study on Autonomy* (Washington, D.C.: June 2016). The study observed that IoT devices—such as thermostats, traffic lights, televisions, mini-drones, and vehicles—typically contain these elements. Throughout this report, we will use the term IoT devices. In the context of IoT, actuating—i.e., actuation—is an action that adjusts physical processes such as modifying temperatures or pressures, or changing the position of a physical object.

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

[3] DOD Chief Information Officer, *DOD Policy Recommendations for the Internet of Things (IoT)* (December 2016).

systems.[4] For example, in October 2016, one security incident involving IoT devices received national attention. A distributed denial of service attack, which appears to have used hundreds of thousands of IoT devices—such as Internet-connected cameras and baby monitors—without the users' knowledge, targeted a company that manages Internet infrastructure. The attack reportedly rendered several major websites unavailable throughout the day.[5] Although several DOD components have security responsibilities relating to IoT, no single lead office or organization in DOD is responsible for IoT security, according to DOD officials.

House Report 114-537, accompanying a bill for the National Defense Authorization Act of Fiscal Year 2017, and House Report 114-573, accompanying a bill for the Intelligence Authorization Act of Fiscal Year 2017, included provisions that we assess the security challenges DOD faces that are associated with the IoT.[6] This report (1) addresses the extent to which DOD has identified and assessed security risks related to IoT devices, (2) assesses the extent to which DOD has developed policies and guidance related to IoT devices, and (3) describes other actions that DOD has taken to address security risks related to IoT devices. The scope of this review includes a range of IoT devices, to include wearable fitness devices, portable electronic devices, smartphones, and infrastructure devices, but it excludes weapon systems—such as airplanes and tanks—and intelligence, surveillance, and reconnaissance networks, which could be described as an example of the IoT.[7] In addition, we assessed IoT devices and their related security challenges, and we excluded from our review the back-end processing and analytic infrastructure, such as cloud computing services, that can store and process IoT device data. This is an unclassified version of a sensitive report that we issued in June 2017. This report does not identify

[4] *Worldwide Threat Assessment of the U.S. Intelligence Community*, *Before the House Permanent Select Committee on Intelligence,* 114th Cong. 1 (2016) (statement of the Director of National Intelligence, James R. Clapper).

[5] Major websites affected by the attack include Twitter, Netflix, Spotify, Airbnb, Reddit, Etsy, SoundCloud, and the *New York Times*, among others. Nicole Perlroth, "Hackers Used New Weapons to Disrupt Major Websites across U.S.," *New York Times*, Oct. 21, 2016, accessed Oct. 26, 2016, http://www.nytimes.com/2016/10/22/business/internet-problems-attack.html?_r=0.

[6] H.R. Rep. No. 114-537, at 277 (2016) and H.R. Rep. No. 114-573, at 16 (2016).

[7] DOD officials use the term "cyber physical systems" to refer in part to a weapons platform, such as an aircraft, and its associated cyberspace domain.

specific details of DOD assessments and other actions DOD is taking to address security risks related to IoT devices—information that DOD deemed to be sensitive. Although the information provided in this report is less detailed, it addresses the same objectives as our sensitive report. Also, the overall methodology used for both reports is the same.

To address the extent to which DOD has identified and assessed security risks related to IoT devices, we obtained documentary and testimonial evidence from DOD reports and officials identifying risks and threats related to IoT devices, including infrastructure devices and smartphones. We examined DOD notional threat scenarios that depict potential consequences of compromised IoT devices. Officials in the Office of the Secretary of Defense, the Navy, Joint Force Headquarters-DOD Information Networks, and the Defense Information Systems Agency developed these scenarios. We interviewed DOD officials, including those from the Office of the Secretary of Defense, the military services, the Defense Information Systems Agency, the National Security Agency, and the Defense Advanced Research Projects Agency, and we identified various types of risk assessments that may address IoT devices.[8] We examined the focus areas of these assessments and determined whether they examined IoT devices. We compared these assessments with DOD criteria on mission assurance and operations security, including cybersecurity operations best practices for IoT devices and the requirement to conduct surveys every 3 years, respectively.[9]

To assess the extent to which DOD has developed policies and guidance related to IoT devices, we reviewed policies and guidance that DOD currently uses for IoT devices. We interviewed officials from the Office of the Secretary of Defense, the Joint Staff, the military services, the Defense Information Systems Agency, U.S. Cyber Command, the Defense Intelligence Agency, the National Security Agency, and the Defense Logistics Agency to identify types of IoT devices that are covered by policy and guidance, as well as any gaps in policies and guidance where security risks may not be addressed. Federal internal control standards require that management evaluate security threats to

[8] For the purposes of this report, we refer to military services as including the Army, Navy, Marine Corps, and Air Force. The U.S. Coast Guard, although a military service, was not included in the scope of our review.

[9] Assessment criteria can be found in: Chairman of the Joint Chiefs of Staff, *2015 DOD Mission Assurance Assessment Benchmarks* (2015), and DOD Directive 5205.02E, *DOD Operations Security (OPSEC) Program* (June 20, 2012).

information technology and periodically review policies and procedures for continued effectiveness in addressing related risks; accordingly, we asked officials whether the department was addressing risks related to IoT devices. We also looked at areas where departmental policies and guidance may not yet be adopted by DOD components.

To describe other actions that DOD has taken to address security risks related to IoT devices, we reviewed documentary and testimonial evidence gathered from DOD and military service officials to describe other ongoing efforts to address and mitigate security risks related to IoT devices.

We conducted this performance audit from June 2016 to July 2017 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

Definition of the IoT

While DOD does not have a standard, department-wide definition of the IoT, the department has identified a number of existing definitions of it. As noted previously, a 2016 Defense Science Board study defined the IoT as the set of Internet Protocol-addressable devices that interact with the physical environment, noting that "IoT devices typically contain elements for sensing, communications, computational processing, and actuation."[10] The study identified that IoT devices span a range of complexity and size, including thermostats, traffic lights, televisions, mini-drones, and full-size vehicles. A 2016 DOD Chief Information Officer policy paper on the IoT cited a definition from a non-DOD organization. According to this definition, the IoT consists of two foundational things: 1) the Internet itself, and 2) semi-autonomous devices (the "things") that leverage inexpensive computing, networking, sensing, and actuating capabilities in uniquely identified implementations to sense the physical world and act on it. Such

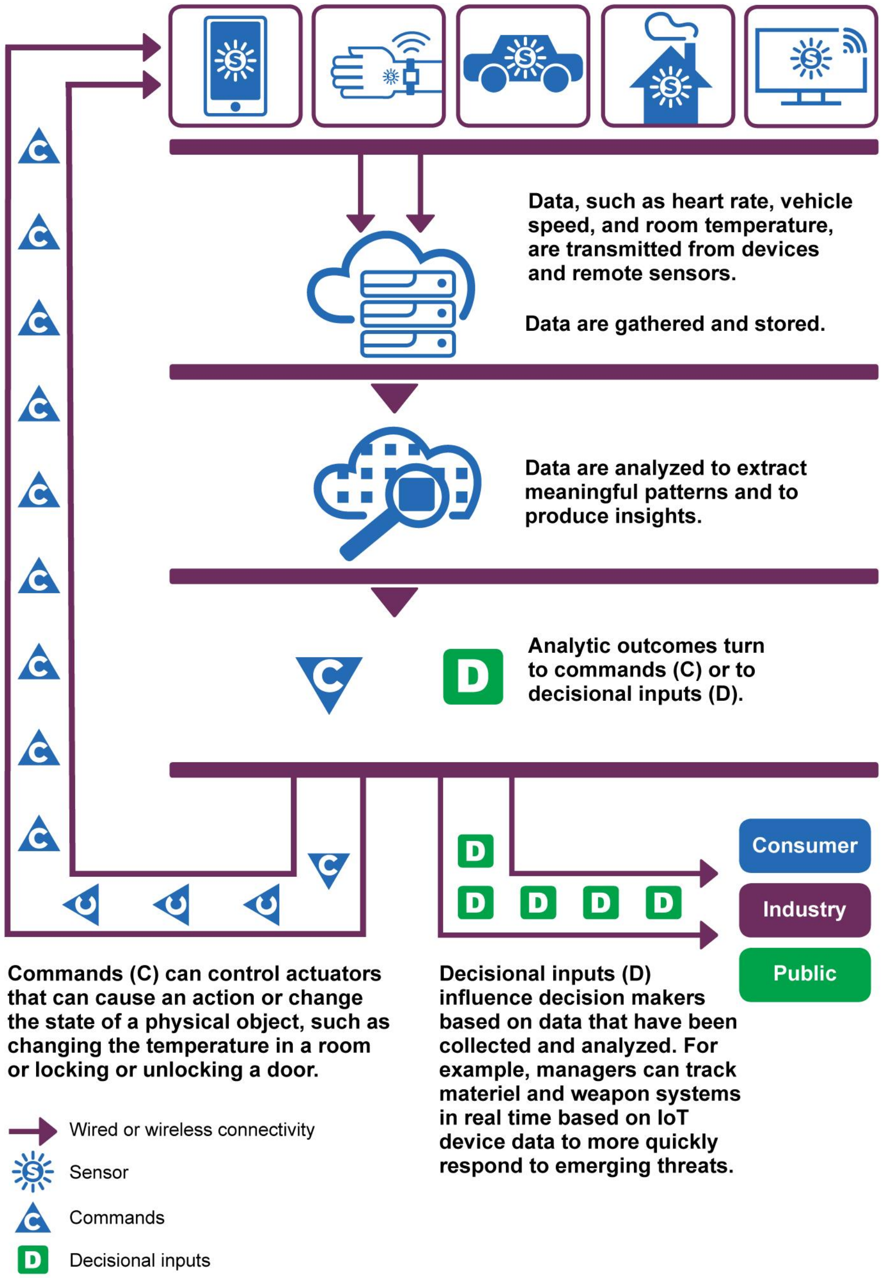
[10] Defense Science Board, *Summer Study on Autonomy*, 87.

devices have the capability to connect to the Internet, being Internet Protocol-based, but may also be deployed in stand-alone Internet Protocol networks.[11] These DOD IoT definitions describe devices having the characteristics of sensing, communicating (or networking), computing (or processing), and actuating, and all leveraging the Internet Protocol.

Figure 1 depicts typical data flows from a range of IoT devices—smartphones, smart watches, cars, buildings, and televisions—where data are collected, transmitted, and analyzed before leading to commands back to the devices or inputs to decision makers. Consumers and senior leaders in industry or public-sector organizations, such as DOD, can potentially act on IoT device data.

[11] DOD Chief Information Officer, *DOD Policy Recommendations for the Internet of Things (IoT)*. DOD cites the Institute of Electrical and Electronics Engineers definition for IoT.

Figure 1: Data from Internet of Things (IoT) Devices Enable Actions and Decisions



Data, such as heart rate, vehicle speed, and room temperature, are transmitted from devices and remote sensors.

Data are gathered and stored.

Data are analyzed to extract meaningful patterns and to produce insights.

Analytic outcomes turn to commands (C) or to decisional inputs (D).

Commands (C) can control actuators that can cause an action or change the state of a physical object, such as changing the temperature in a room or locking or unlocking a door.

Decisional inputs (D) influence decision makers based on data that have been collected and analyzed. For example, managers can track materiel and weapon systems in real time based on IoT device data to more quickly respond to emerging threats.

Source: GAO adapted from Goodman, 2015. | GAO-17-668

Notes: (1) Figure is adapted from the following publication: Ellen P. Goodman (Rapporteur), The Aspen Institute, *The Atomic Age of Data: Policies for the Internet of Things*, Report of the 29th Annual Aspen Institute Conference on Communications Policy (Washington, D.C.: 2015). The license is available here: http://creativecommons.org/licenses/by-nc/3.0/us/ (2) Figure is intended to provide an overview but may not display the full complexity of data flows over DOD networks or all DOD cybersecurity protocols and devices. According to DOD officials, IoT data may move around networks unencrypted and be used by many different types of actors.

Prior GAO Reports Addressing IoT Security Challenges

In a 2016 report, we provided a primer on the IoT that highlighted key benefits of IoT devices, categories of devices, a future outlook for IoT, and security challenges posed by the devices.[12] We reported that security vulnerabilities in many IoT devices can arise for several reasons, including (1) a lack of security standards addressing unique IoT needs; (2) a lack of better incentives for developing secure devices; and (3) the decreasing size of such devices—which limits the computational power that is currently available to implement security protections. The primer cites reports of wireless medical devices being taken over and controlled; of a widespread wireless standard for IoT devices used in smart energy being compromised; and of gas stations' tank-monitoring systems having no passwords, thereby potentially exposing the pumps to a risk of being shut down. These security challenges could potentially impact DOD hospitals and facility energy and fuel systems where managers may consider using or deploying IoT devices.

In May 2017, we issued a technology assessment on the IoT that defined the concept of the IoT, described its uses, highlighted its benefits, and discussed its potential implications, including security challenges.[13] We reported that adoption of the IoT across the different sectors has amplified the challenge of designing and implementing effective security controls by bringing the potential effects of poor security into homes, factories, and communities. In addition, the technology assessment noted a security risk whereby unauthorized individuals or organizations might gain access to these devices and use them for potentially malicious purposes, including fraud or sabotage. The lack of attention to security in designing IoT devices and the predominant use of cloud computing to provide connectivity with these devices pose unique security challenges. These challenges have direct implications for DOD as the department

[12] GAO, *Data and Analytics Innovation: Emerging Opportunities and Challenges*, GAO-16-659SP (Washington, D.C.: Sept. 20, 2016). See appendix IV, "A Brief Primer on the Internet of Things."

[13] GAO-17-75. In the report, we define IoT as the concept of connecting and interacting through a network with a broad array of objects or devices, such as fitness trackers, cameras, door locks, thermostats, vehicles, or jet engines.

considers how to develop and deploy these devices. As cyber threats grow increasingly sophisticated, the need to manage and bolster the cybersecurity of IoT products and services is increasingly critical, according to our technology assessment. According to the assessment, while many industry-specific standards and best practices address information security, standards and best practices that are specific to IoT technologies are either still in development or not widely adopted. Any device that is connected to the Internet is at risk of being compromised if it does not have adequate access controls.

DOD Responsibilities Relating to the IoT

According to DOD officials, no one specific DOD office or entity is responsible for IoT security. Instead, various DOD organizations have roles and responsibilities related to IoT security risks. For example,

- Office of the DOD Chief Information Officer is charged with developing the department’s cybersecurity policy and guidance, as well as policy regarding the continuous monitoring of DOD information technology. The DOD Chief Information Officer has issued instructions on cybersecurity, a risk management framework for DOD information technology, and the use of Internet-based capabilities to collect, store, and disseminate information.
- Within the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, the Office of the Assistant Secretary of Defense for Energy, Installations, and Environment oversees the cybersecurity of industrial control systems on DOD’s facilities—systems that contain IoT devices—and establishes design criteria for these systems that include cybersecurity requirements.[14]
- Office of the Under Secretary of Defense for Intelligence establishes and oversees the implementation of policies and procedures for the conduct of DOD operations security, physical security, and

[14] For purposes of this report, industrial control systems are computer-controlled systems that monitor or operate physical utility infrastructure, among other things. The term “industrial control systems” is a general one that encompasses several types of control systems—including supervisory control and data acquisition systems, distributed control systems, and other control system configurations—often found in the industrial sectors and critical infrastructures, such as electricity, water, and natural gas.

information security.[15] The office has established policy calling for all DOD missions, programs, functions, and activities to be protected by an operations security program.

- Office of the Principal Cyber Advisor to the Secretary of Defense is responsible for overall supervision of cyber activities related to, among other things, defense of DOD networks, including oversight of policy and operational considerations.
- Joint Staff provides guidance on mission assurance assessments—installation-level assessments that integrate information on asset criticality, area-specific hazards and threats, and vulnerabilities to be exploited—and consolidates reporting. The assessments should include benchmarks for the cybersecurity of wireless and portable electronic devices.
- Military services and DOD agencies are to conduct assessments and surveys of their operations security. Additionally, military services and DOD agencies are to delegate responsibilities for mission assurance assessments and to ensure that information technology under their authority complies with the department’s risk management framework.
- Defense Information Systems Agency provides security guidance for DOD-owned smartphones and wireless systems. Command Cyber Readiness Inspection teams conduct oversight and assess implementation of this guidance, according to DOD officials.

[15] In DOD Directive 5205.02E, *DOD Operations Security (OPSEC) Program*, DOD defines operations security, in part, as a process of identifying critical information and analyzing friendly actions to: identify those actions that can be observed by adversary intelligence systems, determine vulnerabilities that these adversary systems might obtain that could be pieced together to derive critical information, determine which of these represent an unacceptable risk, and then select countermeasures to eliminate or reduce the risk to friendly actions.

DOD Has Identified Security Risks with IoT Devices and Begun to Examine Them in Its Assessments, but Operations Security Surveys Are Not Being Conducted

DOD Has Identified Security Risks with IoT Devices and Developed Notional Threat Scenarios

DOD documents and officials identified numerous security risks with IoT devices—as highlighted in table 1—that can generally be divided into risks with the devices themselves and risks with the devices' operational implications.[16]

[16] This table may not identify all of DOD's IoT security risks but is intended to capture key risks cited by DOD—including the Defense Science Board, the DOD Chief Information Officer, the Defense Intelligence Agency, and the Joint Staff. We also interviewed several non-DOD organizations to corroborate and discuss IoT security concerns, including the Internet Society, the National Institute of Standards and Technology, and the Office of the Director of National Intelligence. They generally reinforced the security risks in the table.

Table 1: Internet of Things (IoT) Security Risks Identified by Department of Defense (DOD)

	Security Risks[a]	Description of Concern
Device Risks	Supply Chain Threat	The manufacturing origin of IoT devices and related components poses a significant concern. Adversarial countries like China and Russia could embed “exploits,” or malicious software, into the hardware of chips and other components used in IoT devices, such as smart meters, to collect and transmit data.
	Limited Encryption	Limited encryption in the hardware of IoT devices or the collection and transmission of unencrypted data poses a significant concern. IoT devices have not been designed to facilitate deployment of the latest cryptographic algorithms and protocols, thus posing a range of potential risks, to include eavesdropping, unauthorized access, and device tampering.
	Poor Security in Device Design	Current IoT devices have limited security in the design of their hardware and software, including chip design and cybersecurity software. With little built-in security, IoT devices could be compromised without the user’s knowledge.
	Poor Password Management or Authentication	Poor password management or authentication protocols could lead to DOD industrial control systems or personal IoT accounts being compromised or manipulated by outside hackers.
	Patch or Upgrade Deficiencies	As the number of IoT devices increases, the probability of missing—or not implementing—a security upgrade or patch increases, and some devices may not be patchable at all. In addition, a device could be kept in service longer than it is scheduled to receive security or management updates, which at least one DOD component refers to as a “zombie device.” Any of these situations could lead to potentially vulnerable or exploitable devices by which adversaries could gain unauthorized access.
Operational Risks	Rogue Applications[b]	Some device applications—such as gaming applications—could be installed on personal or even DOD smartphones or other devices, which then take pictures or record the user’s locations. Such functionality of rogue applications could pose security implications for DOD personnel or facilities.
	Adverse Impacts of Devices on Operations Security[c]	IoT devices, including personal smartphones, can tag a person’s location—known as geo-tagging—which presents implications for operations security. Officials from three services noted the lack of awareness among their personnel over IoT device capabilities in their environment and the need for behavioral changes.
	Rogue Wireless Devices[b] and Insider Threat[d]	An increase in the number of IoT devices could significantly increase DOD’s vulnerability to cyber collection. Rogue wireless devices planted by an insider threat or intentionally placed by service personnel (and then compromised) could collect sensitive information or send out data on industrial control systems for purposes of espionage.
	Expansion of Attack Surface	The expansion of IoT devices will significantly increase the number of points at which any network can be attacked. IoT devices would provide more attack vectors into a network and a potential platform for massive, distributed attacks.

Security Risks[a]	Description of Concern
Unauthorized Communication of Information to Third Parties	Some IoT devices could by design collect and send data back to commercial providers, such as third-party help desks, and DOD components may have little insight into the Internet destinations of such data.

Source: GAO analysis of DOD information. | GAO-17-668

[a] This table may not identify all of DOD's IoT security risks but is intended to capture key risks cited by DOD—including the Defense Science Board, the DOD Chief Information Officer, the Defense Intelligence Agency, and the Joint Staff.

[b] DOD officials use the term "rogue" in referring to applications and wireless devices that could be used for malicious purposes even though the applications or wireless devices by themselves are not malicious in nature.

[c] DOD defines operations security in part as a process of identifying critical information and analyzing friendly actions to identify those actions that can be observed by adversary intelligence systems, determine vulnerabilities that these adversary systems might obtain that could be pieced together to derive critical information, determine which of these represent an unacceptable risk, and then select countermeasures to eliminate or reduce the risk to friendly actions.

[d] Insider threats can include DOD personnel working directly with adversaries to collect information or DOD personnel unintentionally assisting adversaries through their inattention to cybersecurity (e.g., poor cyber hygiene) or other actions.

IoT devices pose numerous risks by how they are designed, manufactured, and configured. According to DOD officials, there is little incentive for manufacturers to design security functions into the software or hardware of their products, resulting in little thought or effort given to security.[17] A DOD Chief Information Officer policy paper also states that IoT devices may be subverted during their manufacture and distribution at various points in the supply chain—thereby rendering the cyber attacker's job easier.[18] With respect to IoT configuration, a DOD report in 2016 notes that IoT devices are often sold with old and unpatched software that can lead to the device being exploited as soon as it is taken out of the box.[19] Poor password management is another cybersecurity risk. According to the DOD report, a majority of IoT cloud services allow the user to choose weak passwords—such as "1234"—and, in some cases, prevent the user from using strong passwords.

[17] In a House Energy and Commerce Committee hearing, *Understanding the Role of Connected Devices in Recent Cyber Attacks*, on November 16, 2016, two of the key witnesses also discussed the lack of security in the design and manufacturing of IoT devices, and how manufacturers have not yet had to factor the costs of cybersecurity into devices. According to DOD officials, the department should coordinate with other federal departments and the commercial sector to develop standards for IoT devices.

[18] DOD Chief Information Officer, *DOD Policy Recommendations for the Internet of Things (IoT)*.

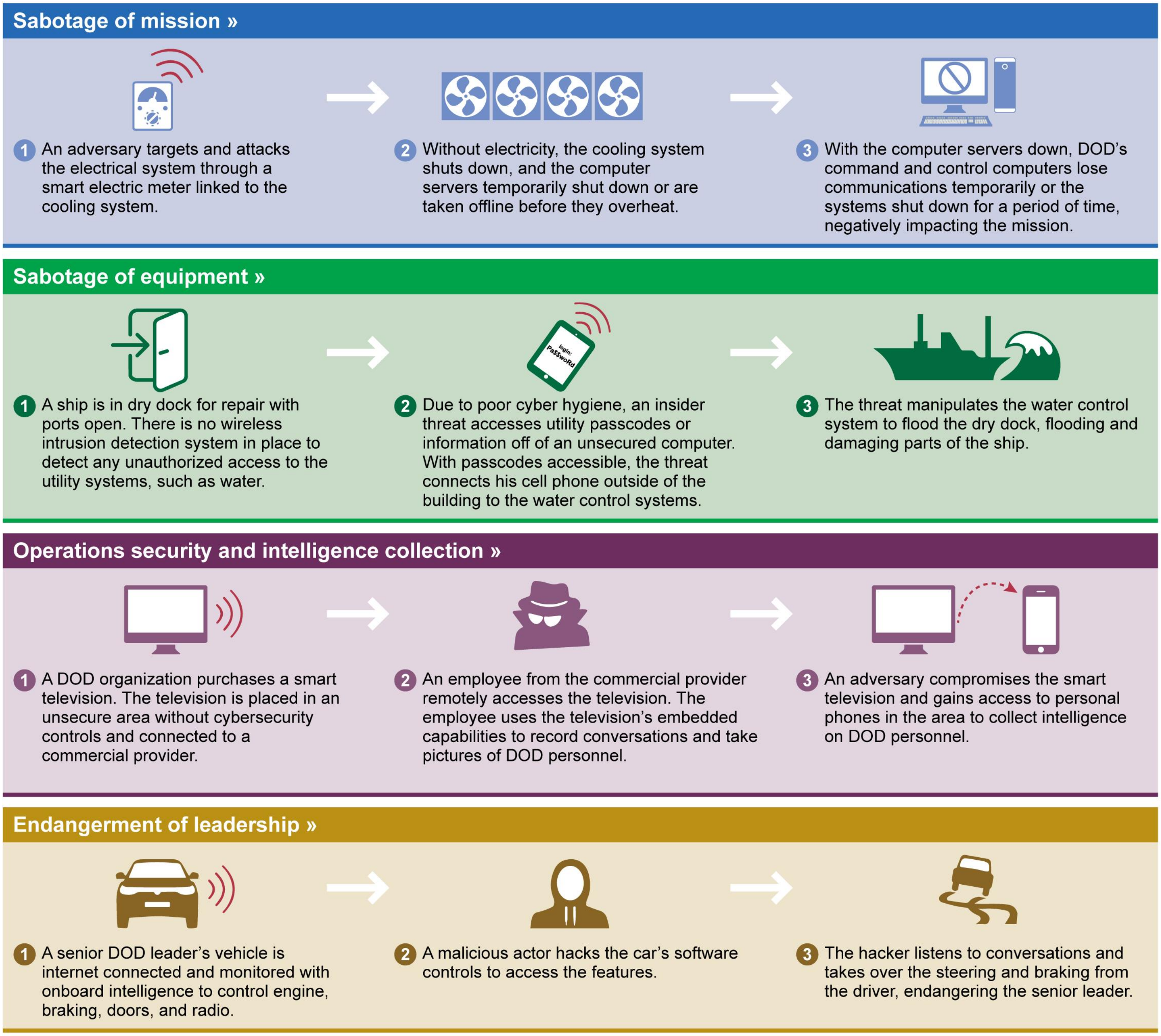
[19] Joint Service Provider, Pentagon Computer Incident Response Team, *Insecurity in the Internet of Things (IoT)* (July 21, 2016).

Given their functionality and capabilities, IoT devices also pose security risks with their operational implications. DOD officials told us that rogue wireless devices in secure areas could provide a pathway for adversaries to collect classified or sensitive information. For example, a cell phone could be concealed and "pocket dialed" such that ambient conversations are recorded or transmitted. Similar to rogue wireless devices, rogue applications also pose risks. According to a DOD report, in 2016 a smartphone gaming application was released that makes use of the global positioning system and the camera of the device on which it is installed.[20] The report cautions that installing the game may lead to the application gaining full access to a user's email account. Whether on personal or DOD-issued devices, the potential of such applications to collect location and photographic data on DOD personnel or units and communicate this data to third parties has raised DOD operations security risks. DOD's 2016 *DOD Policy Recommendations for the Internet of Things (IoT)* also laid out operations security implications of IoT devices, particularly with the expanded aggregation of information. Specifically, it discussed how information collected through various IoT devices and then aggregated could inform adversaries about DOD capabilities or deployments. For example, an adversary could gather information related to which people were present or which organizations were working overtime.

The department has also identified notional threat scenarios that exemplify how these security risks could adversely impact DOD operations, equipment, or personnel. DOD documents and officials from a number of organizations—including the Office of the Secretary of Defense, Joint Force Headquarters-DOD Information Networks, and the Navy—discussed with us a number of notional threat scenarios. Figure 2 highlights a few examples of these scenarios.

[20] Joint Service Provider, *Insecurity in the Internet of Things (IoT)*, 17-19.

Figure 2: Notional Internet of Things (IoT) Scenarios Identified by Department of Defense (DOD)



Sabotage of mission »

1 An adversary targets and attacks the electrical system through a smart electric meter linked to the cooling system.

2 Without electricity, the cooling system shuts down, and the computer servers temporarily shut down or are taken offline before they overheat.

3 With the computer servers down, DOD's command and control computers lose communications temporarily or the systems shut down for a period of time, negatively impacting the mission.

Sabotage of equipment »

1 A ship is in dry dock for repair with ports open. There is no wireless intrusion detection system in place to detect any unauthorized access to the utility systems, such as water.

2 Due to poor cyber hygiene, an insider threat accesses utility passcodes or information off of an unsecured computer. With passcodes accessible, the threat connects his cell phone outside of the building to the water control systems.

3 The threat manipulates the water control system to flood the dry dock, flooding and damaging parts of the ship.

Operations security and intelligence collection »

1 A DOD organization purchases a smart television. The television is placed in an unsecure area without cybersecurity controls and connected to a commercial provider.

2 An employee from the commercial provider remotely accesses the television. The employee uses the television's embedded capabilities to record conversations and take pictures of DOD personnel.

3 An adversary compromises the smart television and gains access to personal phones in the area to collect intelligence on DOD personnel.

Endangerment of leadership »

1 A senior DOD leader's vehicle is internet connected and monitored with onboard intelligence to control engine, braking, doors, and radio.

2 A malicious actor hacks the car's software controls to access the features.

3 The hacker listens to conversations and takes over the steering and braking from the driver, endangering the senior leader.

Source: GAO analysis of Department of Defense (DOD) information. | GAO-17-668

The first notional IoT scenario, the "sabotage of mission," illustrates a few security risks that could adversely impact DOD operations. The increase of IoT devices used to monitor and control DOD infrastructure could increase the number of attack points through which a network or system could be attacked. Many of these devices are insecure because of a limited ability to patch and upgrade devices, or due to poor security design. As a result, the successful penetration of a smart electrical meter could lead to cascading effects that negatively impact an industrial control system and degrade an ongoing mission. In the second notional IoT scenario, “sabotage of equipment,” the combination of poor password management and an insider threat could lead to unauthorized access to a utility system, such as a water system in a dry dock. The insider threat could then manipulate the water control system to flood the dry dock and damage the ship, according to Navy officials. The third notional IoT scenario, “operations security and intelligence collection,” illustrates the adverse impacts on operations security that can emerge from smart televisions. The scenario involves a television with limited cybersecurity controls being targeted by commercial providers or adversaries to collect information for malicious purposes. The fourth notional IoT scenario, the “endangerment of leadership,” depicts how an adversary could exploit a car equipped with IoT capabilities. Here, an adversary—for example exploiting poor security in the car’s devices—could hack a senior DOD official’s car to monitor conversations, take control of car functions, or endanger the lives of senior DOD leaders in the car.[21]

[21] GAO has previously reported on cybersecurity issues that could impact passenger safety in modern vehicles. See GAO, *Vehicle Cybersecurity: DOT and Industry Have Efforts Under Way, but DOT Needs to Define Its Role in Responding to a Real-world Attack*, GAO-16-350 (Washington, D.C.: Mar. 24, 2016).

Mission Assurance and Intelligence Community Assessments Have Examined Security Risks with IoT Devices, but Operations Security Surveys Are Not Being Conducted

While DOD has conducted some assessments to examine security risks with IoT devices, threat-based comprehensive operations security surveys (hereinafter referred to as "operations security surveys") that could examine such risks are not being conducted.[22] DOD requires different types of assessments to protect DOD information residing on and outside the department's networks. Some of these assessments can be used to identify and examine security risks related to IoT devices.[23] Such assessments include mission assurance assessments, specific threat assessments from the intelligence community—such as the Defense Intelligence Agency's April 2016 *Threats via the Internet of Things*—and operations security surveys.[24]

Mission Assurance Assessments Have Been Conducted

According to DOD Directive 3020.40, *Mission Assurance*, DOD component heads are responsible for implementing the mission assurance process and developing assessments.[25] Mission assurance assessments are installation-level assessments that integrate information on asset criticality, area-specific threats, and vulnerabilities.[26] According to the concept of operations, the mission assurance assessments should examine, among other things, security risks related to infrastructure devices. The *2015 DOD Mission Assurance Assessment Benchmarks*

[22] DOD's "threat-based comprehensive operations security survey" is also referred to as an "operations security survey" or an "operations security external assessment," according to an official in the Under Secretary of Defense for Intelligence overseeing operations security for DOD.

[23] For purposes of this report, we reviewed assessments that could include IoT devices already deployed or could identify the devices' broad challenges. We did not review DOD assessments of IoT devices that may have occurred as part of the department's acquisition process.

[24] Defense Intelligence Agency, *Threats via the Internet of Things* (Apr. 27, 2016)(S//NF).

[25] DOD Directive 3020.40, *Mission Assurance (MA)* (Nov. 29, 2016).

[26] Chairman of the Joint Chiefs of Staff, *Mission Assurance Assessments Concept of Operations* (Apr. 28, 2016).

lays out specific cybersecurity operations benchmarks, or best practices, that mission assurance assessment teams can use to examine and address security risks related to IoT devices.[27] Some of these benchmarks include: (1) implementing security policies and configurations to ensure secure wireless access into the networks, and taking measures to prevent unauthorized wireless access; (2) conducting vulnerability scans; (3) determining the extent to which remote access is allowed or necessary; and (4) checking on the current configuration information for all industrial control system components.

To date, DOD has conducted a number of mission assurance assessments.[28] Three of the four military services—the Army, Navy, and Marine Corps—conducted these assessments and identified cybersecurity risks related to IoT devices on critical infrastructure. While the Air Force did not conduct any assessments in 2016, the service plans to conduct mission assurance assessments in 2017, according to service officials. These officials noted that their assessments will have a limited focus on devices. A 2015 assessment conducted on an Army facility detected cybersecurity vulnerabilities with its IoT devices. The assessment identified how an adversary could hack into industrial control systems' wireless devices, leading to cascading effects and mission degradation. Additionally, the cybersecurity vulnerabilities of IoT devices in this mission assurance assessment were linked to the benchmarks. Navy and Marine Corps mission assurance assessments also contained recommendations to address IoT cybersecurity vulnerabilities, such as unauthorized communication of information to third parties, rogue wireless devices, and poor security design in the devices. Regarding the unauthorized communication of information to third parties, Marine Corps officials expressed concern over the potential capture of electronic data from a base and transmission of the data to unknown individuals or entities. Some mission assurance assessments recommended discontinuing remote access to systems where possible, implementing wireless intrusion detection systems to detect unauthorized devices, implementing a configuration management process, and conducting vulnerability scans.

[27] Chairman of the Joint Chiefs of Staff, *2015 DOD Mission Assurance Assessment Benchmarks* (2015).

[28] Mission assurance assessments are conducted by DOD components. Military services to date have conducted mission assurance assessments on a sample of installations.

Intelligence Community Assessments Have Been Conducted

Assessments from the intelligence community have also identified cybersecurity risks related to IoT devices. For example, officials from the Office of the Director of National Intelligence published an essay on challenges with IoT in which they noted that IoT devices present a rich target for attackers and pose a range of potential risks, including eavesdropping and unauthorized access.[29]

Operations Security Surveys Have Not Been Conducted

According to DOD Directive 5205.02E, *DOD Operations Security Program,* DOD components must conduct operations security surveys, at a minimum, every 3 years.[30] Also, DOD's *Operations Security Program Manual* 5205.02-M requires a threat analysis that includes identifying potential adversaries and their associated capabilities to collect, analyze, and exploit critical information as an essential step in the operations security process.[31] This could potentially include information collected by IoT devices. The Under Secretary of Defense for Intelligence is also required to report annually to the Secretary of Defense on the status of the DOD operations security program. According to DOD officials, IoT devices pose significant risks to operations security. Officials cited the geolocation capability of some IoT devices as a particular concern—specifically, how the location of troops or personnel could be revealed. Another concern is the ability to use IoT devices to clandestinely record conversations. Military service and agency officials cited smart televisions as an example of an IoT device that could secretly record conversations of DOD personnel.

[29] "The Darkness of Things: Anticipating Obstacles to Intelligence Community Realization of the Internet of Things Opportunity," *JSCoRE,* vol. 3, no. 1 (2015)(TS//SI//NF).

[30] According to DOD Directive 5205.02E, *DOD Operations Security (OPSEC) Program*, DOD components are also required to conduct annual operations security assessments. According to an official overseeing DOD's operations security program, however, these annual assessments do not specifically address IoT devices.

[31] DOD Manual 5205.02-M, *DOD Operations Security (OPSEC) Program Manual* (Nov. 3, 2008).

DOD Has Policies and Guidance for IoT Devices, but Gaps Remain

DOD has a number of policies as well as guidance for IoT devices, including wearable devices, portable electronic devices, smartphones, and infrastructure devices. Some gaps remain, however, with respect to how DOD addresses security risks associated with IoT in its policies and guidance.

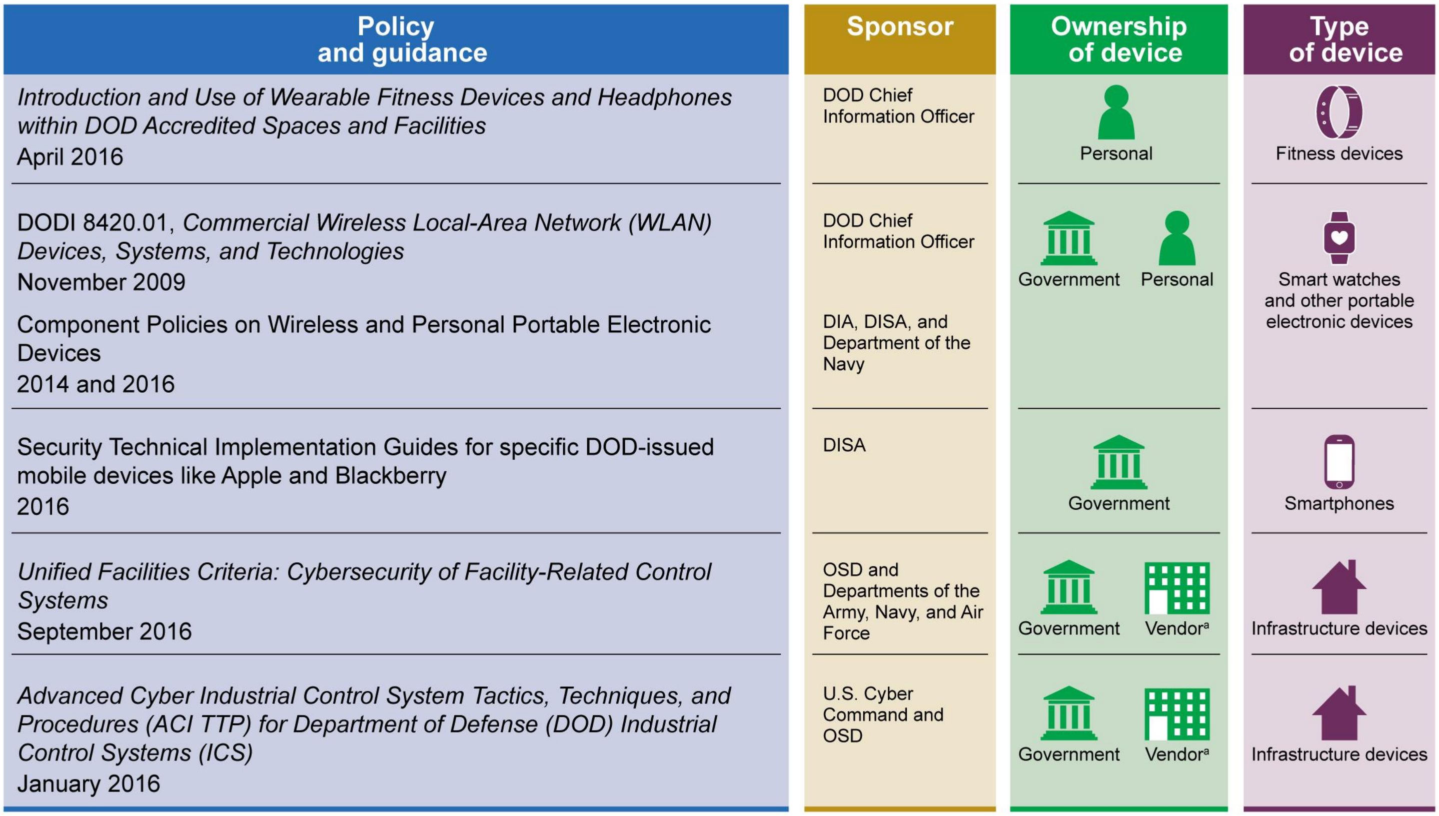
DOD Has Policies and Guidance for IoT Devices

DOD has issued a number of policies and guidance for IoT devices, including personal wearable fitness devices, portable electronic devices, smartphones, and infrastructure devices associated with industrial control systems.[32] Generally, these policies and guidance apply across the department's components. Additionally, many of DOD's policies and guidance address IoT devices based on areas where classified information is processed, and where it is not. Some military services and agencies have issued additional policy and guidance, such as on personal wearable fitness devices and portable electronic devices.

Figure 3 highlights examples of existing DOD policies and guidance for different types of IoT devices. The figure also lists the DOD sponsor of the policy or guidance, the owner of the device, and the type of device for which the policy or guidance applies. This list may not include all department-wide or component policies and guidance on IoT devices but is intended to show a range of policies and guidance on IoT devices.

[32] The Defense Intelligence Agency defines a portable electronic device, in part, as any easily transportable electronic device that has a capability to record, copy, store, or transmit data, digital images, video, or audio. Examples of a portable electronic device include pagers, cellular telephones, radios, personal digital assistants (e.g., iPad), digital audio devices (e.g., iPod), cameras, camcorders, electronic book readers (e.g., Kindle, Nook), and electronic watches (e.g., smart watches).

Figure 3: Examples of Department of Defense (DOD) Policies and Guidance on Types of Internet of Things (IoT) Devices[b]



Policy and guidance	Sponsor	Ownership of device	Type of device
Introduction and Use of Wearable Fitness Devices and Headphones within DOD Accredited Spaces and Facilities April 2016	DOD Chief Information Officer	Personal	Fitness devices
DODI 8420.01, *Commercial Wireless Local-Area Network (WLAN) Devices, Systems, and Technologies* November 2009	DOD Chief Information Officer	Government Personal	Smart watches and other portable electronic devices
Component Policies on Wireless and Personal Portable Electronic Devices 2014 and 2016	DIA, DISA, and Department of the Navy		
Security Technical Implementation Guides for specific DOD-issued mobile devices like Apple and Blackberry 2016	DISA	Government	Smartphones
Unified Facilities Criteria: Cybersecurity of Facility-Related Control Systems September 2016	OSD and Departments of the Army, Navy, and Air Force	Government Vendor[a]	Infrastructure devices
Advanced Cyber Industrial Control System Tactics, Techniques, and Procedures (ACI TTP) for Department of Defense (DOD) Industrial Control Systems (ICS) January 2016	U.S. Cyber Command and OSD	Government Vendor[a]	Infrastructure devices

DIA	Defense Intelligence Agency
DISA	Defense Information Systems Agency
DOD	Department of Defense
OSD	Office of the Secretary of Defense

Source: GAO analysis of Department of Defense (DOD) information. | GAO-17-668

[a] According to DOD officials, DOD criteria or procedures may or may not apply depending on the contract requirements with vendors.

[b] This list may not include all department-wide or component policies and guidance on IoT devices but is intended to show a range of policies and guidance on IoT devices.

Personal Wearable Fitness Devices

The DOD Chief Information Officer issued a DOD-wide policy on personal wearable fitness devices (e.g., step counting, heart rate monitoring).[33] Other DOD components—including at least two military services and the

[33] DOD Chief Information Officer Memorandum, *Introduction and Use of Wearable Fitness Devices and Headphones within DOD Accredited Spaces and Facilities* (Apr. 21, 2016).

National Security Agency—have issued similar guidance on these personal devices. The DOD Chief Information Officer policy addresses the use of personally owned (or government-furnished) devices that meet certain requirements in areas where classified information is stored, processed, or transmitted—authorizing these devices in DOD facilities up to the “top secret” level. The policy prohibits devices with photographic, video recording, or microphone or audio recording capabilities, and requires that wireless or connectivity capabilities be disabled.

Portable Electronic Devices

The DOD Chief Information Officer issued a DOD instruction on portable electronic devices able to connect to DOD unclassified and classified wireless local area networks.[34] This instruction identifies a minimum set of security measures, such as antivirus software, encryption, and personal firewalls that must be present in unclassified wireless local area network-enabled portable electronic devices. Several DOD components—including the Defense Information Systems Agency, the Defense Intelligence Agency, and the Department of the Navy—have also issued policies and guidance on these devices. For example, Defense Intelligence Agency employees and visitors must not use video, wireless, photographic, or other recording capabilities of any personally owned portable electronic devices within any agency spaces unless approved in advance for special events (e.g., promotion ceremonies conducted in common areas).[35] Generally, personally owned portable electronic devices with photographic, video recording, audio recording, or wireless transmission capabilities are prohibited in areas where classified information is processed and in other restricted areas.

Smartphones

The Defense Information Systems Agency has issued a number of policies as well as guidance that apply to DOD-owned smartphones, including mobile Security Requirements Guides and Security Technical

[34] DOD Instruction 8420.01, *Commercial Wireless Local-Area Network (WLAN) Devices, Systems, and Technologies* (Nov. 3, 2009). The instruction does not apply to a number of technologies, such as cellular technologies (e.g., 2.5/3/4G cellular systems), some wireless personal area networking standards (e.g., Bluetooth, ZigBee), receive-only pagers, and global positioning system receivers.

[35] Defense Intelligence Agency Instruction 8460.002, *Portable Electronic Devices* (May 1, 2014).

Implementation Guides for specific smartphones (e.g., Apple, Blackberry, and Samsung).[36] For example, the Security Technical Implementation Guides state that department personnel should disable their phones from: 1) data transfers with the Bluetooth capability on DOD's Blackberry phones; 2) data storage in the iCloud on DOD's Apple phones; and 3) voice dialing on DOD's Apple phones.[37]

Infrastructure Devices

DOD has department-wide policy and guidance that addresses infrastructure devices (e.g., smart electric meters) within industrial control systems.[38] The *Unified Facilities Criteria: Cybersecurity of Facility-Related Control Systems* lays out criteria for the inclusion of cybersecurity in the design of control systems down to the device level.[39] For example, at the IoT device level, some of these cybersecurity controls include (a) the avoidance of wireless communications to the greatest extent possible; (b) the implementation of authentication between devices, if possible; and (c) the avoidance of mobile code—i.e., code that is downloaded and executed without explicit user action. Additionally, the *Advanced Cyber Industrial Control System Tactics, Techniques, and Procedures (ACI TTP) for Department of Defense (DOD) Industrial Control Systems (ICS)* offers guidance and identifies procedures that include infrastructure devices.[40] This guidance identifies device anomalies that could indicate a cyber incident, specific detection procedures to assess the anomaly, and

[36] See, for example, Defense Information Systems Agency, *Mobile Policy Security Requirements Guide,* version 1, release 2 (July 26, 2013); and Defense Information Systems Agency, *Blackberry BES 12.3.x MDM Security Technical Implementation Guide*, version 1, release 1 (May 9, 2016).

[37] The department also gives specific guidance in its End User License Agreement for DOD mobile devices, including the following: (a) Public or hotel Wi-Fi hotspots are not allowed; (b) Global Positioning System is available for use [but] can only be used with approved applications and must be turned off when not in use; and (c) third party email accounts are not authorized.

[38] For our purposes, when referring to infrastructure devices, we generally refer to the lowest level of Internet Protocol-based devices found in industrial control systems. Examples include air handler controller, chiller controller, or electric meter. See earlier footnote for definition of industrial control system we are using.

[39] DOD, Unified Facilities Criteria (UFC) 4-010-06: *Unified Facilities Criteria: Cybersecurity of Facility-Related Control Systems* (Sept. 19, 2016).

[40] U.S. Cyber Command and Office of the Secretary of Defense, *Advanced Cyber Industrial Control System Tactics, Techniques, and Procedures (ACI TTP) for Department of Defense (DOD) Industrial Control Systems (ICS),* version 1.0 (January 2016).

procedures to recover electronic devices, including removing and replacing the device.

Existing DOD Policies and Guidance Do Not Clearly Address Some IoT Risks

DOD policies highlight the importance of protecting and securing DOD information from any potential adversaries. DOD Directive 8000.01, *Management of the Department of Defense Information Enterprise,* states that information is considered a strategic asset to DOD and must be safeguarded, appropriately secured and shared, and made available to authorized personnel to the maximum extent allowed by law, policy, and mission requirements.[41] Similarly, DOD Directive 5205.02E, *DOD Operations Security (OPSEC) Program,* directs that DOD personnel maintain essential secrecy of information that would be useful to adversaries, and that countermeasures are employed to deny adversaries any potential indicators that reveal critical information about DOD missions. Federal internal control standards also require that management evaluate security threats to information technology, which can come from both internal and external sources, and periodically review policies and procedures for continued relevance and effectiveness in addressing related risks.[42] For example, the federal standards note that external threats are particularly important for entities dependent on telecommunications networks and the Internet, and that continual effort is required to address these risks.

Policies and Guidance Do Not Address Certain DOD-acquired IoT Devices and Applications

DOD officials told us that existing DOD policies and guidance do not clearly address security risks relating to smart televisions, and particularly

[41] DOD Directive 8000.01, *Management of the Department of Defense Information Enterprise (DOD IE)* (Mar. 17, 2016). DOD defines information as any knowledge that may be communicated or documentary material, regardless of its physical form or characteristics, that is owned by, is produced by or for, or is under the control of the U.S. government.

[42] Office of Management and Budget Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control* (Jul. 15, 2016) notes that managers should consider GAO reports, among other sources of information, in identifying and correcting internal control deficiencies. Also, GAO, *Standards for Internal Control in the Federal Government*, GAO-14-704G (Washington, D.C.: September 2014), 54, 56.

smart televisions in unsecure areas. Officials from military services and other DOD components described smart televisions as a risk to operations security due, in part, to the ability of commercial providers to access the devices remotely—potentially eavesdropping on conversations or sending recordings of these conversations to third parties.[43] Although they acknowledged the need for them, Navy and Marine Corps officials stated that they do not have service-wide policies addressing cybersecurity controls for smart televisions. Officials from Joint Force Headquarters-DOD Information Networks highlighted the potential to "hop" (i.e., gain access) from smart televisions to personal smartphones in close proximity and thereby possibly gain access to non-DOD networks—potentially leading to the collection of data on DOD personnel.

Additionally, DOD officials affirmed that existing DOD policies and guidance do not clearly address security risks of applications installed on DOD-issued mobile devices. These risks include rogue applications and the unauthorized communication of data to third parties. For example, these officials highlighted the need for policies that could lead to the automatic removal of unauthorized applications from DOD mobile devices or restrictions on the number of parties to whom data are transmitted from an application. DOD officials confirmed that one gaming application—an example of a rogue application—was downloaded on some unclassified DOD-issued phones.[44] Similarly, a DOD report further identifies the dangers of downloading certain applications and unwittingly granting third parties access to a host of personal information on one's own phone.[45] According to a Defense Information Systems Agency official, other mobile applications will likely be downloaded with similar security implications unless the policy recommendations noted above are implemented.

[43] A Defense Science Board's report noted that the microphones of some IoT devices have been hijacked to eavesdrop on conversations without the knowledge of their owners. See Defense Science Board, *Summer Study on Autonomy*, page 89 (June 2016).

[44] As discussed previously in this report, some device applications could be installed on personal or DOD smartphones, which then take pictures or record the user's locations. Such functionality of rogue applications—as DOD uses the term—could pose security implications for DOD personnel or facilities. DOD officials leverage the term "rogue" in referring to applications and wireless devices that could be used for malicious purposes even though the applications or wireless devices by themselves are not malicious in nature.

[45] Joint Service Provider, *Insecurity in the Internet of Things (IoT)*, 17-18.

Core Security Policies Do Not Address IoT Devices

Core DOD security policies and guidance on cybersecurity, operations security, information security, and physical security do not address IoT devices. First, DOD Instruction 8500.01, *Cybersecurity*, and DOD Instruction 8510.01, *Risk Management Framework (RMF) for DOD Information Technology (IT)*—core DOD policies on cybersecurity—do not provide policy and guidance for IoT devices.[46] Although these instructions may apply to IoT devices that are part of a larger system, they neither focus on these devices nor clearly address security risks specific to these devices. DOD officials acknowledged that these instructions do not focus on IoT devices. Similarly, DOD Chief Information Officer's *DOD Policy Recommendations for the Internet of Things (IoT)* also recommends a number of policy tenets to inform changes to DOD's cybersecurity policies, including encryption of IoT data, monitoring of IoT networks for anomalous traffic, and active management of supply chains for IoT devices.

Second, core DOD policies and guidance on operations security do not address IoT devices.[47] As noted earlier, adverse impacts on operations security is a key security risk that DOD identified with IoT devices. Although these core operations security policy documents refer to Internet-based capabilities and the data collection capabilities of potential adversaries, they do not offer guidance to mitigate the risks to operations security associated with these devices. Additionally, a key DOD official with department-wide oversight over operations security agreed that DOD policy on operations security could be enhanced by providing guidance and focusing on IoT devices, including a taxonomy for such devices.

Third, core DOD policies and guidance we reviewed on information security relating to unclassified DOD information do not address IoT

[46] DOD Instruction 8500.01, *Cybersecurity* (Mar. 14, 2014); and DOD Instruction 8510.01, *Risk Management Framework (RMF) for DOD Information Technology (IT)* (Mar. 12, 2014) (incorporating Change 1, May 24, 2016).

[47] See, for example, DOD Directive 5205.02E, *DOD Operations Security (OPSEC) Program* and DOD Manual 5205.02-M, *DOD Operations Security (OPSEC) Program Manual*.

devices.[48] In a 2017 report, we noted that the rapid adoption of IoT devices, the lack of attention to security in the design phase, and the predominant use of cloud computing to provide connectivity with these devices pose unique information security challenges—challenges that could be mitigated in part with DOD guidance on information security.[49] Lastly, core DOD policies and guidance on physical security do not address IoT devices.[50] For example, in one DOD threat scenario, a malicious actor compromises an Internet-connected car of a DOD senior leader and unlocks the doors to abduct the passengers.[51]

Table 2 below summarizes core DOD security policies and guidance we reviewed that do not address security risks related to IoT devices.

Table 2: Core Department of Defense (DOD) Security Policies and Guidance That Do Not Address Internet of Things (IoT) Devices

Core DOD Security Policies and Guidance That Do Not Address IoT Devices	Security Area
DOD Instruction 8500.01, *Cybersecurity*	Cybersecurity
DOD Instruction 8510.01, *Risk Management Framework (RMF) for DOD Information Technology (IT)*	Cybersecurity
DOD Directive 5205.02E, *DOD Operations Security (OPSEC) Program*	Operations Security
DOD Manual 5205.02-M, *DOD Operations Security (OPSEC) Program Manual*	Operations Security

[48] DOD Manual 5200.01 volume 4, *DOD Information Security Program: Controlled Unclassified Information (CUI)* (Feb. 24, 2012); DOD Instruction 5200.01, *DOD Information Security Program and Protection of Sensitive Compartmented Information (SCI)* (Apr. 21, 2016). Regarding the former, volume 1 is an overview and volumes 2 and 3 of the DOD information security manuals address classified information. We selected volume 4 for review based on the likelihood of IoT devices in unsecure areas and the potential collection of unclassified DOD information. According to volume 4, controlled unclassified information is unclassified information that requires safeguarding or dissemination controls, pursuant to and consistent with applicable law, regulations, and government-wide policies.

[49] GAO-17-75.

[50] DOD 5200.08-R, *Physical Security Program* (Apr. 9, 2007) (incorporating change 1, May 27, 2009); DOD Instruction 5200.08, *Security of DoD Installations and Resources and the DOD Physical Security Review Board (PSRB)* (Dec.10, 2005) (incorporating change 3, Nov. 20, 2015). According to the former document, the physical security program is that part of security concerned with active and passive measures designed to prevent unauthorized access to personnel, equipment, installations, information, and to safeguard them against espionage, sabotage, terrorism, damage, and criminal activity.

[51] DOD Chief Information Officer, *DOD Policy Recommendations for the Internet of Things (IoT)*, C-3.

Core DOD Security Policies and Guidance That Do Not Address IoT Devices	Security Area
DOD Instruction 5200.01, *DOD Information Security Program and Protection of Sensitive Compartmented Information (SCI)*	Information Security
DOD Manual 5200.01, Volume 4, *DOD Information Security Program: Controlled Unclassified Information (CUI)*	Information Security
DOD Instruction 5200.08, *Security of DOD Installations and Resources and the DOD Physical Security Review Board (PSRB)*	Physical Security
DOD 5200.08-R, *Physical Security Program*	Physical Security

Source: GAO analysis of DOD information. | GAO-17-668

DOD Does Not Have a Policy to Implement Procedures for Infrastructure Devices

DOD has developed guidance and detailed procedures for defending industrial control systems against cyber attacks. As noted previously, DOD's *Advanced Cyber Industrial Control System Tactics, Techniques, and Procedures (ACI TTP) for Department of Defense (DOD) Industrial Control Systems (ICS)* offers guidance to DOD components and identifies procedures for infrastructure devices, including procedures to assess device anomalies and to recover devices that may have been targeted in cyber attacks. According to U.S. Cyber Command officials, the procedures were tested and validated over the course of 2 years, and U.S. Cyber Command also trained and tested the procedures with Navy personnel over a 2-week period to assess their effectiveness. Although the procedures were found to be effective, DOD does not have a policy that directs the implementation of these procedures throughout the department, according to DOD officials. For example, a DOD installations official cited the need to modify existing and future contracts with vendors of utility services to ensure that these cybersecurity procedures would be put in place.[52] Further, Navy and Air Force officials stated that their services do not have a defined plan in place to implement the advanced cyber industrial control system tactics, techniques, and procedures. Navy officials expressed their intent to fully adopt these procedures; however, they cited a current lack of resources and the strain on system operators—who are more focused on non-security issues—as reasons for not yet having implemented the procedures.

[52] Asked about whether contractors would be involved in implementing the advanced cyber industrial control system tactics, techniques, and procedures, Navy officials affirmed that the vendor contract would have to specify the contractor's role and responsibilities in the procedures. If not in the contract, contractors would not have to implement the procedures.

DOD Has Taken Other Actions to Address Security Risks Related to IoT Devices

In addition to the assessments, policies, and guidance discussed above, DOD has taken other actions to address IoT-related security risks. These ongoing efforts include an inventory of systems that incorporate IoT devices, the establishment of forums to discuss DOD IoT policies, and the research of IoT security issues.

- **Inventory of industrial control systems effort:** In March 2016, the Office of the Assistant Secretary of Defense (Energy, Installations, and Environment) directed the military departments and certain other DOD components to develop plans to implement cyber security controls on their facility industrial control systems, including devices and sensors.[53] All of the military departments drafted and submitted implementation plans or a strategy to the Office of the Assistant Secretary of Defense (Energy, Installations, and Environment) by February 2017. After the initial inventory phase, DOD components are to make their control systems resilient to cyber threats and to implement a continuous monitoring process to respond to emerging threats. The department's goal is to implement cybersecurity controls on the most critical control systems by the end of fiscal year 2019. These actions would be consistent with the National Defense Authorization Act for Fiscal Year 2017 and our recommendation in a prior report, which also requires DOD to take actions on the cybersecurity of its industrial control systems.[54]

[53] Office of the Assistant Secretary of Defense (Energy, Installations, and Environment) Memorandum*, Managing Cyber Risks to Facility-Related Control Systems* (Mar. 31, 2016) directs the military departments and certain other DOD components to conduct control system inventories and to include associated sensors and controllers used to monitor and control real property. The initial inventory is to focus on critical assets.

[54] GAO, *Defense Infrastructure: Improvements in DOD Reporting and Cybersecurity Implementation Needed to Enhance Utility Resilience Planning*, GAO-15-749 (Washington, D.C.: July 23, 2015) recommended that DOD address challenges related to inventorying industrial control systems. We found that, as of February 2015, none of the military services had a complete inventory of existing industrial control systems. Also, the National Defense Authorization Act for Fiscal Year 2017, Pub. L. No. 114-328, § 1650 (2016), requires DOD to submit a plan for the evaluation of the cyber vulnerabilities of its critical infrastructure and initiate a pilot program to assess the feasibility of applying new methodologies to, among other things, improve the defense of control systems against cyber attacks. DOD is to complete and submit a report on its pilot program by the end of 2019.

- **IoT Forum:** According to officials in the Office of the DOD Chief Information Officer, the office has established an informal IoT working group for DOD officials working on IoT issues. The group has attended IoT workshops and developed a paper on the IoT. The group authored and published the policy paper *DOD Policy Recommendations for the Internet of Things (IoT)* in December 2016 to raise awareness of IoT issues. As noted previously, the report discusses the definition of the IoT, the benefits and cybersecurity risks of IoT devices, potential IoT threat scenarios, and DOD policy tenets for addressing the IoT. According to an official in the Office of the DOD Chief Information Officer, their next steps are to establish an IoT community of interest and to produce another IoT report that focuses on DOD component responsibilities and more detailed policy analysis.
- **Research and testing efforts:** The Defense Advanced Research Projects Agency has a few ongoing research programs that relate to IoT security issues. The Leveraging the Analog Domain for Security program seeks to develop new cyber techniques in digital devices by monitoring their analog emissions (e.g., radio waves, sound waves, micro-power changes) and is projected to continue through December 2019. By studying analog signals radiating from IoT devices, they intend to better monitor IoT devices and detect deviations from normal device behavior to provide protection for DOD networks. Additionally, the Vetting Commodity Information Technology Software and Firmware program aims to develop checks for broad classes of malicious features and dangerous flaws in software and firmware. The program includes the IoT and other devices and is projected to continue through September 2017. The program seeks to address the department’s need to ensure that the devices and equipment it procures—much of it produced overseas—do not contain hidden code or malware; this could help address the supply chain risk noted previously.

Conclusions

The IoT and IoT devices represent the wave of the future for the global economy, from infrastructure to public services to consumer use. DOD will likely be involved in using these devices for the foreseeable future. However, IoT devices pose numerous security challenges that need to be addressed, both in specific instances and as part of a holistic approach to risk management in the information age. DOD has made some progress in addressing the security challenges we identify in this report, including: (1) identifying a number of IoT security risks and notional threat scenarios; (2) examining security risks of IoT devices by conducting assessments on critical infrastructure; (3) developing policies and guidance for IoT devices; and (4) establishing ongoing efforts, such as research programs, to mitigate the security risks with these devices. DOD could capitalize on this progress by further addressing challenges we found in the following areas: the lack of operations security surveys that could identify and mitigate security risks of IoT; insufficient DOD policies and guidance for specific IoT devices and applications of concern (e.g., smart televisions and smartphone applications); and the need for DOD core security policies (e.g., cybersecurity, operations security, physical security, information security) that provide clear guidance on the IoT or IoT devices. By addressing these challenges, DOD could better ensure that it is identifying security issues with IoT devices and more effectively safeguarding and maintaining the security of DOD information.

Recommendations for Executive Action

The Under Secretary of Defense for Intelligence, in coordination with the DOD Chief Information Officer, the Under Secretaries of Defense for Policy; Acquisition, Technology, and Logistics; and Personnel and Readiness; and with military service and agency stakeholders, should conduct operations security surveys that identify IoT security risks and protect DOD information and operations, in accordance with DOD guidance, or address operations security risks posed by IoT devices through other DOD risk assessments.

The Principal Cyber Advisor, in coordination with the DOD Chief Information Officer; the Under Secretaries of Defense for Policy; Intelligence; Acquisition, Technology, and Logistics; and Personnel and Readiness; and with military service and agency stakeholders, should

- Review and assess existing departmental security policies and guidance—on cybersecurity, operations security, physical security, and information security—that may affect IoT devices; and
- Identify areas where new DOD policies and guidance may be needed—including for specific IoT devices, applications, or procedures—and where existing security policies and guidance can be updated to address IoT security concerns.

Agency Comments and Our Evaluation

We provided a draft of this report to DOD and the Office of the Director of National Intelligence. DOD provided written comments, in which it concurred with our two recommendations. DOD’s written comments are reprinted in their entirety in appendix II. DOD also provided technical comments, which we incorporated into the report where appropriate. The Office of the Director of National Intelligence did not provide technical comments.

DOD concurred with our recommendation to conduct operations security surveys that identify IoT security risks and protect DOD information and operations, in accordance with DOD guidance, or address operations security risks posed by IoT devices through other DOD risk assessments. The department stated that it will take action in accordance with its existing policies for operations security.

DOD concurred with our recommendation to review and assess existing departmental security policies and guidance—on cybersecurity, operations security, physical security, and information security—that may affect IoT devices; and to identify areas where new DOD policies and guidance may be needed—including for specific IoT devices, applications, or procedures—and where existing security policies and guidance can be updated to address IoT security concerns. The department stated that it has already begun work in this area and should complete a review of its policies and guidance affected by IoT by the end of the fourth quarter, fiscal year 2017. DOD also stated that updates to address IoT will be done as part of the department’s policy update process.

We are sending copies of this report to the appropriate congressional committees, the Secretary of Defense, the Under Secretary of Defense for Intelligence, DOD's Principal Cyber Advisor, the Under Secretaries of Defense for Policy; Acquisition, Technology, and Logistics; and Personnel and Readiness; DOD's Chief Information Officer, and the Director of National Intelligence. In addition, the report is available at no charge on the GAO website http://www.gao.gov.

If you or your staff has any questions about this report, please contact me at (202) 512-9971 or kirschbaumj@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix III.

Joseph W. Kirschbaum
Director, Defense Capabilities and Management

List of Committees

The Honorable John McCain
Chairman
The Honorable Jack Reed
Ranking Member
Committee on Armed Services
United States Senate

The Honorable Richard Burr
Chairman
The Honorable Mark Warner
Vice Chairman
Select Committee on Intelligence
United States Senate

The Honorable Mac Thornberry
Chairman
The Honorable Adam Smith
Ranking Member
Committee on Armed Services
House of Representatives

The Honorable Devin Nunes
Chairman
The Honorable Adam Schiff
Ranking Member
Permanent Select Committee on Intelligence
House of Representatives

Appendix I: Objectives, Scope, and Methodology

The objectives of this report were to (1) address the extent to which Department of Defense (DOD) has identified and assessed security risks related to Internet of Things (IoT) devices; (2) assess the extent to which DOD has developed policies and guidance related to IoT devices; and (3) describe other actions DOD has taken to address security risks related to IoT devices.

The scope of this review includes a range of IoT devices, to include wearable fitness devices, portable electronic devices, smartphones, and infrastructure devices, but it excludes weapon systems—such as airplanes and tanks—and intelligence, surveillance, and reconnaissance networks, which could be described as an example of the IoT. In addition, we assessed IoT devices and their related security challenges, and we excluded from our review the back-end computing and analytic infrastructure, such as computer servers, that can store and process IoT device data.

To address the extent to which DOD has identified and assessed security risks related to IoT devices, we reviewed DOD reports on IoT, including reports from the Defense Science Board, the Office of the DOD Chief Information Officer, the Defense Intelligence Agency, and Joint Staff, that identified broad security risks with IoT devices.[1] We also interviewed officials from a number of organizations—including the Office of the Secretary of Defense, Joint Force Headquarters-DOD Information Networks, the military services, the Defense Information Systems Agency, the National Security Agency, the Defense Intelligence Agency, and the Defense Advanced Research Projects Agency—to identify key security risks associated with IoT devices.[2] After these interviews and

[1] These reports included the following: Defense Science Board, *Summer Study on Autonomy* (June 2016); DOD Chief Information Officer, *DOD Policy Recommendations for the Internet of Things (IoT)* (December 2016); Defense Intelligence Agency, *Threats via the Internet of Things* (Apr. 27, 2016); and Joint Service Provider, Pentagon Computer Incident Response Team, *Insecurity in the Internet of Things (IoT)* (July 21, 2016).

[2] Within the Office of the Secretary of Defense, we interviewed officials in the office of the DOD Chief Information Officer, as well as those in the Office of the Under Secretaries of Defense for Acquisition, Technology, and Logistics (Research and Engineering; and Energy, Installations, and Environment); Intelligence; and Policy.

reviews, we grouped identified risks into common categories. We examined DOD notional threat scenarios that depict consequences ensuing from compromised IoT devices. Officials in the Office of the Secretary of Defense, the Navy, the Defense Information Systems Agency, and Joint Force Headquarters-DOD Information Networks developed these scenarios. Through our interviews with organization officials, we identified various types of risk assessments that may address security risks related to IoT devices. We reviewed the focus areas of these assessments and identified whether they examined IoT devices. We compared these assessments against DOD criteria.[3] We collected and analyzed a non-generalizable sample of these assessments to review. For the mission assurance assessments, we requested and received a sample of documents from the services to review. From our request, we received and reviewed a total of 11 mission assurance assessments—2 from the Army, 2 from the Navy, and 7 from the Marine Corps. With respect to intelligence assessments, we requested and received 1 assessment from the Defense Intelligence Agency and 1 from the Office of the Director of National Intelligence—documenting the challenges related to the IoT.

To assess the extent to which DOD has developed policies and guidance related to IoT devices, we interviewed officials from the Office of the Secretary of Defense, the Joint Staff, the military services, the Defense Information Systems Agency, U.S. Cyber Command, the Defense Intelligence Agency, the National Security Agency, and the Defense Logistics Agency to identify current policies and guidance applying to a range of IoT devices, including wearable fitness devices, portable electronic devices, smartphones, and infrastructure devices. We reviewed these policies and guidance—including the DOD Chief Information Officer's *DOD Policy Recommendations for the Internet of Things (IoT)*—and identified their general characteristics, applicability, and focus areas. When we interviewed officials from the organizations noted above, we also asked them whether there are any gaps in policies and guidance for IoT devices, applications, or procedures. We compiled their responses to identify a few commonly cited policy and guidance gaps where security risks may not be addressed. Additionally, we reviewed core DOD security policy documents on cybersecurity, operations security, physical security, and information security (see table 2 in the report) to assess whether

[3] Criteria can be found in: Chairman of the Joint Chiefs of Staff, *2015 DOD Mission Assurance Assessment Benchmarks* (2015) and DOD Directive 5205.02E, *DOD Operations Security (OPSEC) Program* (June 20, 2012).

these documents addressed IoT devices or security risks associated with IoT devices. We used relevant search terms such as “device,” “capabilities,” and “threat” to make these assessments. Federal internal control standards require that management evaluate security threats to information technology and periodically review policies and procedures for continued effectiveness in addressing related risks, so we asked officials whether the department was addressing risks related to IoT devices.

To describe other actions DOD has taken to address security risks related to IoT devices, we interviewed officials from a number of organizations—including the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics; Office of the DOD Chief Information Officer; the National Security Agency; the Defense Advanced Research Projects Agency; the Defense Intelligence Agency; and the military services—and collected documents to identify and describe ongoing efforts and actions to address and mitigate security risks relating to IoT devices. We grouped ongoing efforts they identified into categories, such as research, inventory tasks, forums, and the development of use cases. Due to the limited number of ongoing efforts directly tied to IoT we could identify, we developed a small number of categories—which captured all of these efforts—by distinguishing among the primary focuses of these efforts. These focuses included long-term knowledge building, information collection on assets, intra-departmental collaboration, and the development of threat scenarios or environments.

To address our reporting objectives, we reviewed relevant documents and interviewed knowledgeable officials from the following DOD organizations and offices as identified in table 3.

Table 3: Department of Defense (DOD) Organizations and Offices GAO Interviewed

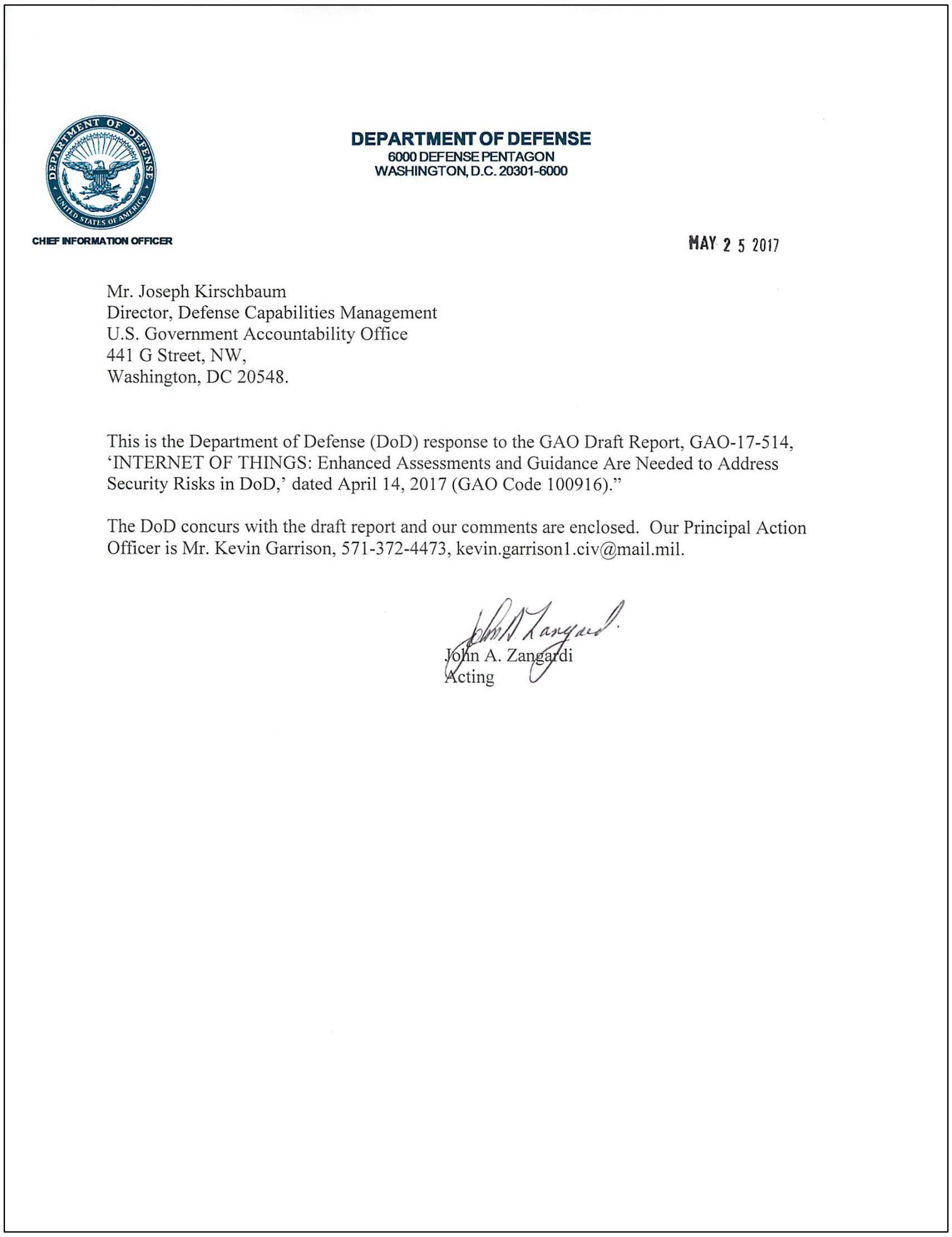
DOD Organizations GAO Interviewed	Sub-organizations or Positions
Office of the Secretary of Defense	DOD Chief Information Officer Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics Office of the Under Secretary of Defense for Policy Office of the Under Secretary of Defense for Intelligence Defense Health Agency
Joint Staff	J3 and J6
U.S. Air Force	Office of the Chief Information Officer Air Force Headquarters A4 Chief, Air Force Operations Security Air Force Security Forces Center, Mission Assurance Assessment team
U.S. Army	Army Headquarters Chief Information Officer Army Headquarters G-3/5/7, Mission Assurance Assessment team Army Medical Command Army Cyber Command Army Operations Security Program Manager
U.S. Navy	Office of the Deputy Chief Information Officer Office of the Chief of Naval Operations N46 Installations Deputy Under Secretary of the Navy for Policy, Security Directorate Naval Operations Security Support Team
U.S. Marine Corps	Headquarters Cyber Directorate Installations and Logistics Information Technology Director Marine Corps Installations Command
U.S. Cyber Command	J3, J5, and J6
Defense Advanced Research Projects Agency	Information Innovation Office
Defense Intelligence Agency	Defense Technology and Long-Range Analysis Office Office of Security
Defense Information Systems Agency	Risk Management Executive DOD Information Networks Inspection Division Joint Force Headquarters-DOD Information Networks
Defense Logistics Agency	J3 and J6
National Security Agency	Office of Security and Counterintelligence Capabilities Directorate

Source: GAO Summary of DOD Organizations and Positions Interviewed. | GAO-17-668

We also interviewed officials from three non-DOD organizations, including the Office of the Director of National Intelligence, the Internet Society, and the National Institute of Standards and Technology. We interviewed the Office of the Director of National Intelligence to gain a non-DOD intelligence community perspective of cyber issues related to IoT devices. We also interviewed the Internet Society to collect insights on IoT issues from a non-governmental organization. Lastly, we interviewed the National Institute of Standards and Technology as they have issued a number of cybersecurity documents, including those that apply to IoT devices.

We conducted this performance audit from June 2016 to July 2017 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: Comments from the Department of Defense



DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

CHIEF INFORMATION OFFICER

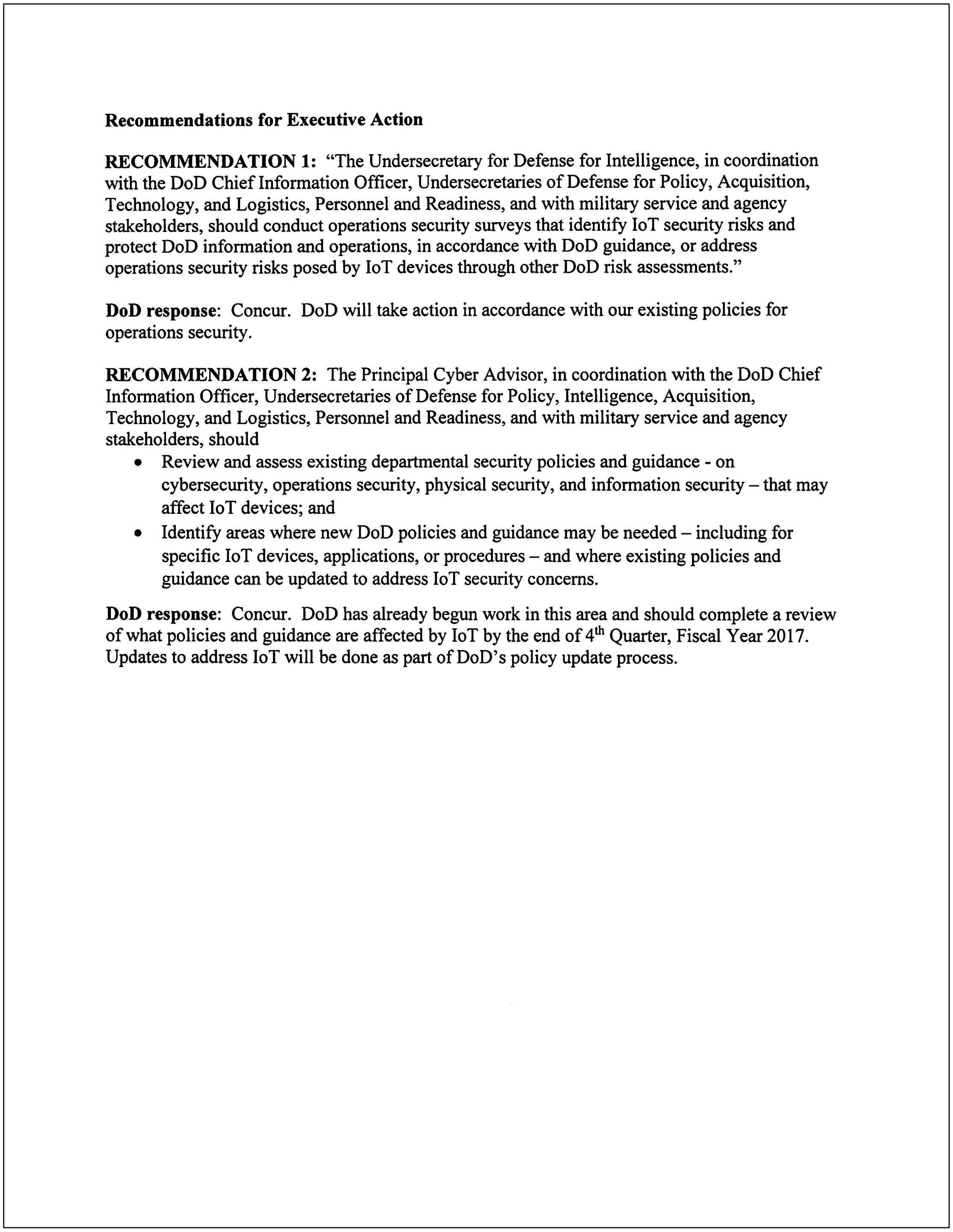
MAY 2 5 2017

Mr. Joseph Kirschbaum
Director, Defense Capabilities Management
U.S. Government Accountability Office
441 G Street, NW,
Washington, DC 20548.

This is the Department of Defense (DoD) response to the GAO Draft Report, GAO-17-514, ‘INTERNET OF THINGS: Enhanced Assessments and Guidance Are Needed to Address Security Risks in DoD,’ dated April 14, 2017 (GAO Code 100916).”

The DoD concurs with the draft report and our comments are enclosed. Our Principal Action Officer is Mr. Kevin Garrison, 571-372-4473, kevin.garrison1.civ@mail.mil.

John A. Zangardi
Acting



Recommendations for Executive Action

RECOMMENDATION 1: "The Undersecretary for Defense for Intelligence, in coordination with the DoD Chief Information Officer, Undersecretaries of Defense for Policy, Acquisition, Technology, and Logistics, Personnel and Readiness, and with military service and agency stakeholders, should conduct operations security surveys that identify IoT security risks and protect DoD information and operations, in accordance with DoD guidance, or address operations security risks posed by IoT devices through other DoD risk assessments."

DoD response: Concur. DoD will take action in accordance with our existing policies for operations security.

RECOMMENDATION 2: The Principal Cyber Advisor, in coordination with the DoD Chief Information Officer, Undersecretaries of Defense for Policy, Intelligence, Acquisition, Technology, and Logistics, Personnel and Readiness, and with military service and agency stakeholders, should

- Review and assess existing departmental security policies and guidance - on cybersecurity, operations security, physical security, and information security – that may affect IoT devices; and
- Identify areas where new DoD policies and guidance may be needed – including for specific IoT devices, applications, or procedures – and where existing policies and guidance can be updated to address IoT security concerns.

DoD response: Concur. DoD has already begun work in this area and should complete a review of what policies and guidance are affected by IoT by the end of 4th Quarter, Fiscal Year 2017. Updates to address IoT will be done as part of DoD's policy update process.

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contact

Joseph W. Kirschbaum, (202) 512-9971 or kirschbaumj@gao.gov

Staff Acknowledgments

In addition to the contact named above, key contributors to this report were Tommy Baril (Assistant Director), Ivelisse Aviles, Tracy Barnes, John Beauchamp, Jennifer Beddor, Robert Breitbeil, Jennifer Cheung, Amie Lesser, and Cheryl Weissman.

Appendix IV: Accessible Data

Data Tables

Data Table for Highlights graphic, Notional Internet of Things (IoT) Scenarios Identified by Department of Defense (DOD)

Operations security and intelligence collection:

1. A smart television is in an unsecure area and connected to a provider.
2. An employee from the provider uses the television to record conversations and take pictures.
3. An adversary accesses personal phones through the television to collect intelligence.

Endangerment of leadership:

1. A DOD leader's vehicle is internet connected with onboard intelligence.
2. A malicious actor hacks the car's software controls to access the features.
3. The hacker listens to conversations and takes control from the driver.

Source: GAO analysis of Department of Defense (DOD) information. | GAO-17-668

Data Table for Figure 1: Data from Internet of Things (IoT) Devices Enable Actions and Decisions

- Data, such as heart rate, vehicle speed, and room temperature, are transmitted from devices and remote sensors.
- Data are gathered and stored.
- Data are analyzed to extract meaningful patterns and to produce insights.
- Analytic outcomes turn to commands (C) or to decisional inputs (D).
- Commands (C) can control actuators that can cause an action or change the state of a physical object, such as changing the temperature in a room or locking or unlocking a door.
- Decisional inputs (D) influence decision makers based on data that have been collected and analyzed. For example, managers can track

materiel and weapon systems in real time based on IoT device data to more quickly respond to emerging threats.

- Wired or wireless connectivity
- Sensor
- Commands

Data Table for Figure 2: Notional Internet of Things (IoT) Scenarios Identified by Department of Defense (DOD)

Sabotage of mission:

1. An adversary targets and attacks the electrical system through a smart electric meter linked to the cooling system.
2. Without electricity, the cooling system shuts down, and the computer servers temporarily shut down or are taken offline before they overheat.
3. With the computer servers down, DOD’s command and control computers lose communications temporarily or the systems shut down for a period of time, negatively impacting the mission.

Sabotage of equipment:

1. A ship is in dry dock for repair with ports open. There is no wireless intrusion detection system in place to detect any unauthorized access to the utility systems, such as water.
2. Due to poor cyber hygiene, an insider threat accesses utility passcodes or information off of an unsecured computer. With passcodes accessible, the threat connects his cell phone outside of the building to the water control systems.
3. The threat manipulates the water control system to flood the dry dock, flooding and damaging parts of the ship.

Operations security and intelligence collection:

1. A DOD organization purchases a smart television. The television is placed in an unsecure area without cybersecurity controls and connected to a commercial provider.

2. An employee from the commercial provider remotely accesses the television. The employee uses the television's embedded capabilities to record conversations and take pictures of DOD personnel.
3. An adversary compromises the smart television and gains access to personal phones in the area to collect intelligence on DOD personnel.

Endangerment of leadership:

1. A senior DOD leader's vehicle is internet connected and monitored with onboard intelligence to control engine, braking, doors, and radio.
2. A malicious actor hacks the car's software controls to access the features.
3. The hacker listens to conversations and takes over the steering and braking from the driver, endangering the senior leader.

Source: GAO analysis of Department of Defense (DOD) information. | GAO-17-668

Data Table for Figure 3: Examples of Department of Defense (DOD) Policies and Guidance on Types of Internet of Things (IoT) Devices

Policy and guidance:

Policy and Guidance	Sponsor	Ownership of Device
Introduction and Use of Wearable Fitness Devices and Headphones within DOD Accredited Spaces and Facilities, April 2016	DOD Chief Information Officer	Personal
DODI 8420.01, Commercial Wireless Local-Area Network (WLAN) Devices, Systems, and Technologies, November 2009	DOD Chief Information Officer	Government and Personal
Component Policies on Wireless and Personal Portable Electronic Devices, 2014 and 2016	DIA, DISA, and Department of the Navy	Government and Personal
Security Technical Implementation Guides for specific DOD-issued mobile devices like Apple and Blackberry, 2016	DISA	Government
Unified Facilities Criteria: Cybersecurity of Facility-Related Control Systems, September 2016	OSD and Departments of the Army, Navy, and Air Force	Government and Vendor

Policy and Guidance	Sponsor	Ownership of Device
Advanced Cyber Industrial Control System Tactics, Techniques, and Procedures (ACI TTP) for Department of Defense (DOD) Industrial Control Systems (ICS), January 2016	U.S. Cyber Command and OSD	Government and Vendor

Type of device:

- Fitness devices
- Smart watches and other portable electronic devices
- Smartphones
- Infrastructure devices
- Infrastructure devices

Abbreviations

DIA	Defense Intelligence Agency
DISA	Defense Information Systems Agency
DOD	Department of Defense
OSD	Office of the Secretary of Defense

Source: GAO analysis of Department of Defense (DOD) information. | GAO-17-668

Agency Comment Letter

Text of Appendix II: Comments from the Department of Defense

Page 1

Mr. Joseph Kirschbaum

Director, Defense Capabilities Management

U.S. Government Accountability Office 441 G Street, NW ,

Washington, DC 20548.

This is the Department of Defense (DoD) response to the GAO Draft Report, GA0- 17-514, 'INTERNET OF THINGS: Enhanced Assessments and Guidance Are Needed to Address Security Risks in DoD,' dated April 14, 20 17 (GAO Code 100916)."

The DoD concurs with the draft report and our comments are enclosed. Our Principal Action Officer is Mr. Kevin Garrison, 571-372-4473, kevin.garr ison1.civ@mail.mil.

Page 2

Recommendations for Executive Action

RECOMMENDATION 1:

"The Undersecretary for Defense for Intelligence, in coordination with the DoD ChiefInformation Officer, Undersecretaries of Defense for Policy, Acquisition, Technology, and Logistics, Personnel and Readiness, and with military service and agency stakeholders, should conduct operations security surveys that identify IoT security risks and protect DoD information and operations, in accordance with DoD guidance, or address operations security risks posed by IoT devices through other DoD risk assessments."

DoD response: Concur.

DoD will take action in accordance with our existing policies for operations security.

RECOMMENDATION 2:

The Principal Cyber Advisor, in coordination with the DoD Chief Information Officer, Undersecretaries of Defense for Policy, Intelligence, Acquisition, Technology, and Logistics, Personnel and Readiness, and with military service and agency stakeholders, should

- Review and assess existing departmental security policies and guidance - on cybersecurity, operations security, physical security, and information security -that may affect IoT devices; and
- Identify areas where new DoD policies and guidance may be needed - including for specific IoT devices, applications, or procedures - and where existing policies and guidance can be updated to address IoT security concerns.

DoD response: Concur.

DoD has already begun work in this area and should complete a review of what policies and guidance are affected by IoT by the end of 4th Quarter, Fiscal Year 2017.

Updates to address IoT will be done as part of DoD's policy update process.

Related GAO Products

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

GAO, Data and Analytics Innovation: Emerging Opportunities and Challenges, GAO-16-659SP (Washington, D.C.: Sep. 20, 2016).

GAO, Defense Infrastructure: Improvements in DOD Reporting and Cybersecurity Implementation Needed to Enhance Utility Resilience Planning, GAO-15-749 (Washington, D.C.: July 23, 2015)

GAO, Vehicle Cybersecurity: DOT and Industry Have Efforts Under Way, but DOT Needs to Define Its Role in Responding to a Real-world Attack, GAO-16-350 (Washington, D.C.: Mar. 24, 2016).

(102074)

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 GAO’s website (http://www.gao.gov). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to http://www.gao.gov and select “E-mail Updates.”

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, http://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, LinkedIn, Twitter, and YouTube.

Subscribe to our RSS Feeds or E-mail Updates. Listen to our Podcasts.

Visit GAO on the web at www.gao.gov and read The Watchblog.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: http://www.gao.gov/fraudnet/fraudnet.htm

E-mail: fraudnet@gao.gov

Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Katherine Siggerud, Managing Director, siggerudk@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

James-Christian Blockwood, Managing Director, spel@gao.gov, (202) 512-4707

U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548