July 2017

INTERNET OF THINGS

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

GAO Highlights

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

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

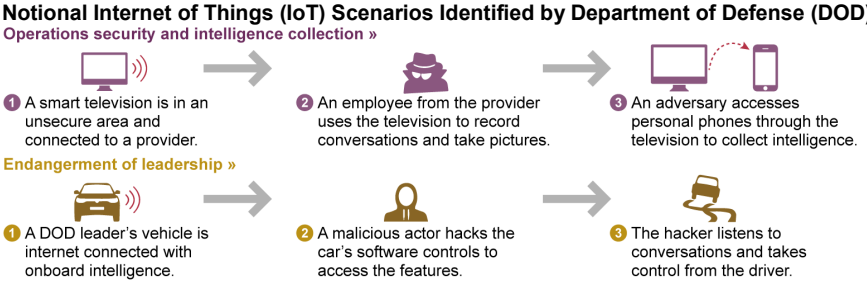
GAO recommends that DOD (1) conduct operations security surveys that could address IoT security risks or address operations security risks posed by IoT devices through other DOD risk assessments; and (2) review and assess its security policies and guidance affecting IoT devices and identify areas, if 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)



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.