December 2014

FEDERAL FACILITY CYBERSECURITY

DHS and GSA Should Address Cyber Risk to Building and Access Control Systems

GAO Highlights

Highlights of GAO-15-6, a report to congressional requesters

Why GAO Did This Study

Federal facilities contain building and access control systems—computers that monitor and control building operations such as elevators, electrical power, and heating, ventilation, and air conditioning—that are increasingly being connected to other information systems and the Internet. The increased connectivity heightens their vulnerability to cyber attacks, which could compromise security measures, hamper agencies' ability to carry out their missions, or cause physical harm to the facilities or their occupants.

GAO's objective was to examine the extent to which DHS and other stakeholders are prepared to address cyber risk to building and access control systems in federal facilities. GAO reviewed DHS's and other stakeholders' authorities to protect federal facilities from cyber attacks; visited selected FPS-protected facilities to determine what stakeholders were doing to address cyber risks to these systems; and interviewed experts about the cyber vulnerability of building and access control systems and related issues. GAO also reviewed GSA's security assessment process and a sample of reports.

What GAO Recommends

GAO recommends that DHS (1) develop and implement a strategy to address cyber risk to building and access control systems and (2) direct ISC to revise its *Design-Basis Threat* report to include cyber threats to building and access control systems. GAO also recommends that GSA assess cyber risk of its building control systems fully reflecting FISMA and its guidelines. DHS and GSA agreed with the recommendations.

View GAO-15-6. For more information, contact Mark L. Goldstein at (202) 512-2834 or goldsteinm@gao.gov or Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

The Department of Homeland Security (DHS) has taken preliminary steps to begin to understand the cyber risk to building and access controls systems in federal facilities. For example, in 2013, components of DHS's National Protection and Programs Directorate (NPPD) conducted a joint assessment of the physical security and cybersecurity of a federal facility. However, significant work remains.

- **Lack of a strategy:** DHS lacks a strategy that: (1) defines the problem, (2) identifies the roles and responsibilities, (3) analyzes the resources needed, and (4) identifies a methodology for assessing this cyber risk. A strategy is a starting point in addressing this risk. The absence of a strategy that clearly defines the roles and responsibilities of key components within DHS has contributed to a lack of action within the Department. For example, no one within DHS is assessing or addressing cyber risk to building and access control systems particularly at the nearly 9,000 federal facilities protected by the Federal Protective Service (FPS) as of October 2014. According to an NPPD official, DHS has not developed a strategy, in part, because cyber threats involving these systems are an emerging issue. By not developing a strategy document for assessing cyber risk to facility and security systems, DHS and, in particular, NPPD have not effectively articulated a vision for organizing and prioritizing efforts to address the cyber risk facing federal facilities that DHS is responsible for protecting.
- **Cyber threat not identified in report for federal agencies:** The Interagency Security Committee (ISC), which is housed within DHS and is responsible for developing physical security standards for nonmilitary federal facilities, has not incorporated cyber threats to building and access control systems in its *Design-Basis Threat* report that identifies numerous undesirable events. An ISC official said that recent active shooter and workplace violence incidents have caused ISC to focus its efforts on policies in those areas first. Incorporating the cyber threat to building and access control systems in the *Design-Basis Threat* report will inform agencies about this threat so they can begin to assess its risk. This action also could prevent federal agencies from expending limited resources on methodologies that may result in duplication.

GSA has not fully assessed the risk of building control systems to a cyber attack in a manner that is consistent with the Federal Information Security Management Act of 2002 (FISMA) or its implementation guidelines. Although GSA has assessed the security controls of these systems, the assessments do not fully assess the elements of risk (e.g., threat, vulnerability, and consequence). GSA also has not yet conducted security control assessments for many of its building control systems. GSA information technology officials said that GSA has conducted security assessments of the building control systems that are in about 500 of its 1,500 FPS-protected facilities and plans to complete the remainder in fiscal year 2015 or when systems are connected to the network or the Internet. Further, our review of 20 of 110 of the security assessment reports that GSA prepared during 2010 to 2014 showed that they were not comprehensive or fully consistent with FISMA implementation guidelines. For example, 5 of the 20 reports we reviewed showed that GSA assessed the building control device to determine if a user's identity and password were required for login but did not assess the system to determine if password complexity rules were enforced. This could potentially lead to weak or insecure passwords being used to secure building control systems.