Highlights

Highlights of GAO-18-95, a report to congressional requesters

October 2017

PHYSICAL SECURITY

NIST and Commerce Need to Complete Efforts to Address Persistent Challenges

Why GAO Did This Study

NIST is the United States' national physical laboratory, which among other matters is responsible for developing measurement standards. In 2017, NIST, located within Commerce, employed approximately 3,500 federal personnel and hosted about 4,000 associates, who include guest researchers and facility users, among others. Assessments in 2015 found issues with NIST's security culture.

GAO was asked to conduct a comprehensive review of the physical security of NIST's campuses. This report examines the extent to which: (1) NIST incorporated key practices to transform the security program and address security vulnerabilities; (2) the security program's organizational structure reflects best practices; and (3) the risk management process aligns with ISC standards.

GAO reviewed risk assessments and related documents; interviewed officials from Commerce and NIST; conducted a generalizable survey of NIST staff; and performed covert vulnerability testing, which provided illustrative examples.

What GAO Recommends

GAO is making four recommendations: NIST should incorporate elements of key practices into its ongoing security efforts; Commerce, in coordination with NIST, should evaluate the current physical security management structure; and Commerce and NIST should both finalize and implement coordinated risk management policies. Commerce concurred with all four recommendations.

View GAO-18-95. For more information, contact Seto J. Bagdoyan at (202) 512-6722 or bagdoyans@gao.gov.

What GAO Found

GAO found that efforts to transform the physical security program at the National Institute of Standards and Technology (NIST) have incorporated some key practices, particularly with regard to leadership commitment to organizational change. For example, GAO estimates that, as of May 2017, 75 percent of staff GAO surveyed believe that NIST leadership places "great" or "very great" importance on security issues. However, staff awareness about security responsibilities varied, in part because of the limited effectiveness of NIST's security-related communication efforts. Additionally, GAO agents gained unauthorized access to various areas of both NIST campuses in Gaithersburg, Maryland, and Boulder, Colorado. GAO found that ongoing efforts do not provide NIST with the tools needed to address security vulnerabilities. By incorporating elements of key practices, including a comprehensive communication strategy, interim milestone dates, and measures to assess effectiveness, NIST will be better positioned to address the security vulnerabilities caused by varied levels of security awareness among employees.

Management of NIST's physical security program is fragmented between the Department of Commerce (Commerce) and NIST. This is inconsistent with the federal Interagency Security Committee's (ISC) physical security best practices, which encourage agencies to centrally manage physical security. Commerce is responsible for overseeing security personnel who implement physical security policies, while NIST manages physical security countermeasures such as access control technology, leading to fragmentation in responsibilities. Before implementing the current organizational structure in October 2015, neither Commerce nor NIST assessed whether it was the most appropriate way to fulfill NIST's physical security responsibilities. Without evaluating management options, the current organizational structure may be creating unnecessary inefficiencies, thereby inhibiting the effectiveness of the security program overall.

To help federal agencies protect and assess risks to their facilities, the ISC developed a risk management process standard (RMP Standard), with which federal agencies, including Commerce, generally must comply. Commerce and NIST most recently completed risk management steps for NIST campuses in 2015 and 2017, but GAO found that their efforts did not fully align with the RMP Standard. Neither Commerce nor NIST used a sound risk assessment methodology, fully documented key risk management decisions, or appropriately involved stakeholders, partly because these requirements were not in existing agency policy. Further, GAO found that Commerce and NIST had overlapping risk management activities, potentially leading to unnecessary duplication. According to officials, Commerce and NIST are separately drafting new risk management policies. Without ensuring that (1) these policies align with the RMP Standard and (2) the NIST policy contains a formal mechanism to coordinate with Commerce, future risk management activities may be limited in their usefulness and duplicative.

This report is a public version of a sensitive report that was also issued in October. Information that Commerce and the Department of Homeland Security deemed sensitive has been omitted.