United States Government Accountability Office

Testimony

Before the Subcommittees on Oversight and Research and Technology, Committee on Science, Space, and Technology, House of Representatives

For Release on Delivery
Expected at 10:00 a.m. ET
Wednesday, October 11, 2017

PHYSICAL SECURITY

NIST and Commerce Need to Complete Efforts to Address Challenges

Statement of Seto J. Bagdoyan, Director, Forensic Audits and Investigative Service

Accessible Version

Chairman LaHood, Chairwoman Comstock, Ranking Members Beyer and Lipinski, and Members of the Subcommittees:

Thank you for the opportunity to discuss our work on the physical security program at the National Institute of Standards and Technology (NIST). NIST is responsible for providing the measurements, calibrations, and quality-assurance techniques that underpin commerce, technological progress, improved product reliability, and manufacturing processes in the United States. In 2017, NIST, located within the Department of Commerce (Commerce), employed approximately 3,500 federal personnel and hosted 4,000 associates, who include guest researchers and facility users, among others.

Recent incidents have raised questions about security vulnerabilities at NIST and the agency's ability to properly secure its physical facilities and assets. Specifically, in July 2015, a federal police officer at the NIST campus in Gaithersburg, Maryland, caused an explosion while attempting to illegally manufacture methamphetamine in a partially vacant laboratory building. In April 2016, an individual unaffiliated with NIST gained unauthorized access to a secured facility at NIST's Boulder, Colorado, campus and subsequently required medical attention. These incidents have also prompted efforts by NIST to transform its security program.

Commerce and NIST currently share responsibilities for ensuring the security of NIST facilities. Specifically, the Office of Security (OSY) within Commerce is responsible for overseeing NIST's Police Services Group (PSG) and contract guards, as well as personnel and information security.[1] NIST's Emergency Services Office manages physical security countermeasures, such as access control technology and closed-circuit televisions. Commerce is also responsible for protecting NIST facilities, assets, and employees from security threats or violent acts, in part by assessing risks to these facilities.

To help federal agencies protect and assess risks to their facilities, the federal Interagency Security Committee (ISC) developed a physical security standard, *The Risk Management Process for Federal Facilities*

[1]Pursuant to 15 U.S.C. § 278e(b), the Secretary of Commerce is authorized to undertake activities related to the care, maintenance, protection, repair, and alteration of NIST buildings and other plant facilities, equipment, and property.

(RMP Standard),[2] with which all federal executive-branch agencies, including Commerce, generally must comply.[3]

My remarks today are based on our report that is being released at this hearing.[4] This report is the public version of a sensitive report that was also issued in October 2017.[5] Specifically, this testimony discusses the extent to which (1) efforts to transform the physical security program at NIST incorporated key practices and addressed security vulnerabilities; (2) the organizational structure of the NIST physical security program reflects best practices; and (3) NIST's risk management process for physical security aligns with ISC standards and best practices.

For our reports, we employed several methods to develop our findings. We conducted a generalizable survey of 506 randomly selected NIST employees and associates to identify common themes related to perspectives about NIST's physical security program. We also conducted covert surveillance and nongeneralizable vulnerability testing at the Gaithersburg and Boulder campuses, and interviewed relevant Commerce and NIST officials. In addition, we compared OSY and NIST's risk management activities performed for both campuses in 2015 and 2017 to the RMP Standard. Additional information on our scope and methodology is available in our October 2017 reports. Our audit work for these reports was performed in accordance with generally accepted

[2]Interagency Security Committee, *The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard* (November 2016). This RMP Standard incorporates the following appendixes as separate documents: Appendix A: *The Design-Basis Threat Report (FOUO)*; Appendix B: *Countermeasures (FOUO)*; and Appendix C: *Child-Care Centers Level of Protection Template (FOUO)*.

[3]The ISC is chaired by the Department of Homeland Security (DHS) and comprises 60 member agencies. The ISC was created pursuant to Executive Order 12977, 60 Fed. Reg. 54411 (Oct. 19, 1995) and subsequently amended by Executive Order 13286, 68 Fed. Reg. 10619 (Feb. 28, 2003). The ISC is housed within DHS's National Protection and Programs Directorate, Office of Infrastructure Protection.

[4]GAO, *Physical Security: NIST and Commerce Need to Complete Efforts to Address Persistent Challenges*, GAO-18-95 (Washington, D.C.: Oct. 11, 2017).

[5]GAO, *Physical Security: NIST and Commerce Need to Complete Efforts to Address Persistent Challenges,* GAO-18-14SU (Washington, D.C.: Oct. 4, 2017). Commerce and DHS deemed some of the information in this report to be sensitive, which must be protected from public disclosure. Therefore, GAO-18-95 omits sensitive information about our investigative methods, as well as specific details regarding security measures, threats, and vulnerabilities, the release of which could pose unintended security risks. Although the information provided in GAO-18-95 is more limited, it addresses the same objectives as the sensitive report and uses the same methodology.

government auditing standards, and our related investigative work was done in accordance with investigative standards prescribed by the Council of the Inspectors General on Integrity and Efficiency.

In summary, we found that

- efforts to transform the physical security program at NIST incorporate some key practices but do not fully address security vulnerabilities;
- the organizational structure of NIST's physical security program does not fully reflect best practices, potentially inhibiting effectiveness; and
- OSY and NIST have taken some steps to align NIST's risk management process with ISC standards but could better coordinate future activities.

We made four recommendations to address these issues, and Commerce agreed with each of the recommendations.

Efforts to Transform the Physical Security Program at NIST Incorporate Some Key Practices but Do Not Fully Address Security Vulnerabilities

Since 2015, NIST and OSY's efforts to transform the physical security program at NIST have incorporated some key practices associated with effective organizational transformations but have not yet addressed others.[6] In particular, leadership has taken steps to improve organizational culture associated with physical security, such as by obtaining independent assessments, developing an Action Plan, and then

[6]We have previously identified key practices of successful large-scale organizational transformations, which include (1) ensuring top leadership drives the transformation; (2) establishing a coherent mission and integrated strategic goals to guide the transformation; (3) focusing on a key set of principles and priorities; (4) setting implementation goals and a timeline; and (5) establishing a communication strategy to create shared expectations and report related progress. We determined that some of the key practices identified in our prior work, such as changing the agency's overall performance management system, did not apply to our assessment, given the status of NIST's ongoing transformation of its physical security program. GAO, *Results-Oriented Cultures: Implementation Steps to Assist Mergers and Organizational Transformations*, GAO-03-669 (Washington, D.C.: July 2, 2003).

initiating a Security Prioritization Sprint (Security Sprint). By taking these steps soon after the security incident at the Gaithersburg campus in July 2015, NIST leadership made a statement about the importance of change and demonstrated a commitment to making change, which are key practices associated with effective organizational transformation. For example, on the basis of our survey, we estimate that as of May 2017 about three-quarters of NIST scientific and technical employees believe that NIST leadership places "great" or "very great importance" on physical security issues, suggesting that leadership has been successful at demonstrating its commitment to security through recent efforts.[7]

Although NIST leadership has taken some steps to transform the organizational culture related to physical security at NIST, these efforts have not fully addressed security vulnerabilities. We found that varied levels of staff awareness about security responsibilities created security vulnerabilities, partly due to the limited effectiveness of NIST's security-related communication efforts. We identified security vulnerabilities through our covert vulnerability testing, during which GAO agents gained unauthorized access to various areas of both NIST campuses.[8] We also identified security vulnerabilities through our survey results. For example, some NIST employees who are not required to complete security training reported having observed colleagues not following certain NIST security policies.[9] In contrast, NIST employees working in highly sensitive facilities, all of whom are required to complete additional mandatory security training, reported significantly fewer observations of colleagues not following NIST security policies. As part of its ongoing Security Sprint, NIST has begun to address these issues through action plans. However, these action plans do not incorporate key practices, such as establishing a communication strategy, interim milestone dates, and measures to assess effectiveness. By incorporating these practices, NIST will be better positioned to effectively address the security vulnerabilities caused by varied levels of security awareness among employees.

[7]We conducted a generalizable survey from March 17, 2017, through May 10, 2017. Our survey reflects the efforts of NIST leadership prior to the Security Sprint, because the initial phase of that effort was not completed until April 2017. During the time frame of the survey, NIST did not take any action related to the Security Sprint report.

[8]The findings from our covert vulnerability testing represent illustrative examples and are not generalizable.

[9]Details related to the specific scenarios and behaviors we asked about, as well as the associated survey results, are provided in the sensitive version of this report, GAO-18-14SU.

In our report released today, we recommend that the NIST Director incorporate elements of key practices into NIST's ongoing security efforts. Commerce agreed with this recommendation.

The Organizational Structure of NIST's Physical Security Program Does Not Fully Reflect Best Practices, Potentially Inhibiting Effectiveness

The organizational structure of NIST's physical security program does not fully reflect best practices, which encourage agencies to centrally manage physical security through a Director of Security or Chief Security Officer. Since 2015, responsibility for physical security at NIST has been split between OSY and NIST, and management of the program has been fragmented.[10] Many of OSY and NIST's responsibilities, however, must be integrated to effectively implement the physical security program. For example, NIST maintains the physical infrastructure required to secure campus perimeters, while the PSG and contract guards patrol and secure the campus. While the best practices indicate that the Director of Security is usually within an agency's internal security office, in the case of NIST, the 2017 American Innovation and Competitiveness Act requires OSY to directly manage the law-enforcement and site-security programs of NIST through an assigned Director of Security for NIST.[11]

Prior efforts by NIST, including the Security Sprint, have noted that the existing organizational structure limits the effectiveness of NIST's security program. However, neither OSY nor NIST evaluated the feasibility of other organizational options for NIST's physical security program before proposing to implement the current structure. Further, despite the findings of the Security Sprint and other assessments, there are no plans to assess whether the current structure is the most appropriate way to fulfill NIST's security requirements. An evaluation could provide the NIST Director and Congress with greater assurance that the current structure is

[10]We have defined fragmentation as those circumstances in which more than one federal agency (or more than one organization within an agency) is involved in the same broad area of national need and opportunities exist to improve service delivery. GAO, *2017 Annual Report: Additional Opportunities to Reduce Fragmentation, Overlap, and Duplication and Achieve Other Financial Benefits*, GAO-17-491SP (Washington, D.C.: Apr. 26, 2017).

[11]Pub. L. No. 114-329, § 113, 130 Stat. 2969 (Jan. 6, 2017).

the most effective and feasible approach to physical security at NIST, or identify whether a consolidated security structure centrally managed by OSY, which would comply with the American Innovation and Competitiveness Act requirements, might better suit NIST's security requirements. Without an evaluation, the structure, which has been in place since October 2015, will likely create unnecessary inefficiencies and competing priorities, and thereby inhibit the effectiveness of the physical security program overall, as well as ongoing efforts to improve the program.

In our report released today, we recommend that the Director of OSY, in coordination with the NIST Director, evaluate the effectiveness of the current security management structure. Commerce agreed with our recommendation.

OSY and NIST Have Taken Some Steps to Align NIST's Risk Management Process with ISC Standards but Could Better Coordinate Future Activities

OSY and NIST's most-recent risk management activities for physical security at NIST's campuses did not fully align with the RMP Standard.[12] Specifically, neither OSY nor NIST used sound risk assessment methodologies, fully documented key risk management decisions, or appropriately involved stakeholders when completing steps in the risk management process in 2015 and 2017. OSY is revising Commerce's department-wide security risk management policy and developing guidance, which could address some issues with OSY and NIST's recent efforts, such as issues with their risk assessment methodologies and documentation of key decisions. In addition, while the draft policy provided to us in July 2017 did not contain specific requirements associated with stakeholder involvement and ISC training, an OSY official stated that such requirements would be included in the final policy. If finalized and implemented as intended, these policy changes and

[12]OSY and NIST performed risk management steps for NIST's Gaithersburg and Boulder campuses in 2015, and NIST performed risk management steps for both campuses from February to May 2017, as part of its Security Sprint. We evaluated these activities against the version of the RMP Standard that was applicable at the time they were performed.

guidance could directly address some of the issues we identified in OSY and NIST's risk management activities (see table 1).

Table 1: Extent to Which the Department of Commerce's (Commerce) Planned Risk Management Policy and Guidance Revisions Would Address Some Issues at the National Institute of Standards and Technology (NIST)

Issue area	2015 Risk management activities	2017 Security Sprint	Can this issue area be addressed by planned revisions to Commerce's policy and guidance?
Risk assessment methodology	Commerce did not use a sound risk assessment methodology.	NIST did not use a sound risk assessment methodology.	Yes[a]
Documentation of key decisions	Commerce did not fully document facility security level (FSL) calculations. NIST did not fully document decisions about countermeasures.	NIST did not fully document review of FSL determinations. NIST did not fully document decisions about countermeasures.	Yes
Stakeholder involvement	Tenant agencies did not document agreement with Commerce's FSL determinations. NIST did not provide other tenant agencies with decision-making authority over recommended countermeasures for its campus in Boulder.	NIST did not provide other tenant agencies with decision-making authority over the FSL determination or recommended countermeasures for its campus in Boulder.	No[b]
Interagency Security Committee (ISC) Risk Management Training	Commerce assessors did not complete ISC training. NIST could not confirm that its decision maker completed ISC training.	NIST's assessors and decision maker did not complete ISC training.	No[c]

Source: GAO analysis of Commerce, NIST, and ISC data. | GAO-18-167T

[a]The draft policy requires assessors to use the ISC's Appendix A: *The Design-Basis Threat Report (FOUO)* when conducting assessments. As of 2016, Appendix A: *The Design-Basis Threat Report (FOUO)* identifies 33 undesirable events, but draft guidance accompanying the draft policy identifies 32 undesirable events. An undesirable event is an incident that has an adverse impact on the facility occupants or visitors, operation of the facility, or mission of the agency. Office of Security (OSY) officials stated that the final policy will require assessors to consider all undesirable events identified by the ISC's standard on the risk management process.

[b]As of July 2017, Commerce's draft policy does not require agencies to establish a facility security committee at multitenant facilities or campuses.

[c]While the draft policy does not contain specific ISC training requirements, an OSY official said that assessors have begun to receive training and it is expected that all assessors will be trained by the end of fiscal year 2018.

Additionally, although OSY and NIST have taken some steps to align NIST's risk management process with the RMP Standard, the two entities did not coordinate their overlapping risk management activities. This could lead to duplicative efforts, hinder potential progress toward

improving NIST's physical security program, and expose the campuses to risks.[13] Because NIST is currently developing its policy for performing its own risk assessments, it has the opportunity to incorporate a mechanism to ensure a high level of coordination with OSY, which could reduce overlapping activities, thereby minimizing the potential for unnecessary duplication.

In our report released today, we recommend that the Director of OSY should ensure that the draft Commerce risk management policy is finalized and implemented in accordance with the ISC's RMP Standard, including requirements for risk assessment methodologies, documentation of key decisions, stakeholder involvement, and training. Additionally, we recommend that the NIST Director should finalize and implement risk management policies that ensure formal coordination between OSY and NIST and align with Commerce's revised risk management policy. Commerce agreed with our recommendations.

Chairman LaHood, Chairwoman Comstock, Ranking Members Beyer and Lipinski, and Members of the Subcommittees, this concludes my prepared remarks. I would be happy to answer any questions that you may have at this time.

GAO Contact and Staff Acknowledgments

For further information regarding this testimony, please contact Seto J. Bagdoyan, (202) 512-6722 or bagdoyans@gao.gov. In addition, contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. Individuals who made key contributions to this testimony are Gabrielle Fagan (Assistant Director); Amber D. Gray (Analyst in Charge); Georgette Hagans; and Elizabeth Kowalewski. Individuals who made key contributions to the report upon which this testimony is based include Elizabeth Dretsch, Justin Fisher, April H. Gamble, James Murphy, Carl Ramirez, and Shana Wallace.

[13]GAO-17-491SP. We have defined overlap as occurring when multiple agencies or programs have similar goals, engage in similar activities or strategies to achieve them, or target similar beneficiaries. We have defined duplication as occurring when multiple agencies or programs engage in the same activities or provide the same services to the same beneficiaries.

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