



October 2017

PHYSICAL SECURITY

NIST and Commerce Need to Complete Efforts to Address Persistent Challenges

This report was revised on March 14, 2018 to clarify information on pages 3, 6, 42, and 43 about the population included in the report's generalizable survey. This clarification had no impact on the conclusions of our report.

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.

PHYSICAL SECURITY

NIST and Commerce Need to Complete Efforts to Address Persistent Challenges

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.

Contents

| | | |
|--------------|--|----|
| Letter | | 1 |
| | Background | 5 |
| | Efforts to Transform the Physical Security Program at NIST Incorporate Some Key Practices but Do Not Fully Address Security Vulnerabilities | 11 |
| | The Organizational Structure of NIST's Physical Security Program Does Not Fully Reflect Best Practices, Potentially Inhibiting Effectiveness | 20 |
| | OSY and NIST Have Taken Some Steps to Align NIST's Risk Management Process with ISC Standards, but Could Better Coordinate Future Activities | 27 |
| | Conclusions | 39 |
| | Recommendations for Executive Action | 40 |
| | Agency Comments | 41 |
| Appendix I | Methods of Survey of National Institute of Standards and Technology Personnel | 42 |
| Appendix II | Comments from the Department of Commerce | 48 |
| Appendix III | GAO Contact and Staff Acknowledgments | 51 |
| Tables | | |
| | 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) | 37 |
| | Table 2: Survey Population, Sample, and Outcomes | 45 |
| Figures | | |
| | Figure 1: Organizational Chart for Managing the National Institute of Standards and Technology's Physical Security Program, July 2017 | 7 |
| | Figure 2: Summary of the Interagency Security Committee's Risk Management Process | 8 |

| | |
|--|----|
| Figure 3: Physical Security Responsibilities at the National Institute of Standards and Technology (NIST), as of July 2017 | 21 |
| Figure 4: Management Structure of the National Institute of Standards and Technology (NIST) Physical Security Program, as of July 2017 | 22 |
| Figure 5: Summary of the Department of Commerce's Documentation of Key Decisions Related to Facility Security Level (FSL) Determinations for National Institute of Standards and Technology Campuses in 2015 | 30 |

Abbreviations

| | |
|-----------------|--|
| CCTV | closed-circuit television |
| Commerce | Department of Commerce |
| DHS | Department of Homeland Security |
| FPS | Federal Protective Service |
| FSC | facility security committee |
| FSL | facility security level |
| GSA | General Services Administration |
| ISC | Interagency Security Committee |
| NIST | National Institute of Standards and Technology |
| NOAA | National Oceanic and Atmospheric Administration |
| NTIA | National Telecommunications and Information Administration |
| OSY | Office of Security |
| PSG | Police Services Group |
| RMP Standard | The Risk Management Process for Federal Facilities |
| SAB | Security Advisory Board |
| Security Sprint | Security Prioritization Sprint |

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



October 11, 2017

The Honorable John Thune
Chairman
Committee on Commerce, Science, and Transportation
United States Senate

The Honorable Lamar Smith
Chairman
Committee on Science, Space, and Technology
House of Representatives

In July 2015, a federal police officer at the National Institute of Standards and Technology (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, was able to gain unauthorized access to a secured facility at NIST's Boulder, Colorado, campus and subsequently required medical attention. These incidents have raised questions about security vulnerabilities and the agency's ability to properly secure its physical facilities and assets, while also prompting efforts to transform NIST's security program.

NIST is a nonregulatory agency within the Department of Commerce (Commerce) 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 fiscal year 2017, NIST's total budget was \$952 million, which includes funding for seven laboratory programs across the Gaithersburg and Boulder campuses.¹ These laboratory programs contain human, physical, and intellectual capital assets.

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

¹The Boulder campus also houses facilities for the National Telecommunications and Information Administration (NTIA) and the National Oceanic and Atmospheric Administration (NOAA).

security.² NIST's Emergency Services Office manages physical security countermeasures, such as door alarms, access control technology, and closed-circuit televisions (CCTV), at the two campuses.

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 (RMP Standard)*,³ with which all federal executive-branch agencies, including Commerce, generally must comply.⁴ Among other things, the RMP Standard includes standards for agencies' facility risk assessment methodologies.

In light of recent security incidents at NIST, you asked us to conduct a comprehensive review of the physical security of NIST's Gaithersburg and Boulder campuses.⁵ This report addresses the following questions:

1. To what extent have efforts to transform the physical security program at NIST incorporated key practices and addressed security vulnerabilities?
2. To what extent does the organizational structure of the NIST physical security program reflect best practices?

²Pursuant 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.

³Interagency 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)*.

⁴The 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.

⁵Physical security involves security-in-depth, which is the use of multiple layers of interdependent systems such as physical barriers, intrusion-detection systems, CCTV surveillance, security guards, access control, lighting, etc. These techniques are designed to detect, deter, delay, or deny unauthorized access to facilities, equipment, and resources.

3. To what extent does NIST’s risk management process for physical security align with ISC standards and best practices?

This report is a public version of a sensitive report issued in October 2017.⁶ Commerce and the Department of Homeland Security (DHS) deemed some of the information in our October report to be sensitive, which must be protected from public disclosure. Therefore, this report omits sensitive information about our investigative methods, as well as specific details regarding security measures, threats, and vulnerabilities, which could pose unintended security risks. This report also omits specific results of a generalizable survey we conducted. Although the information provided in this report is more limited, the report addresses the same objectives as the sensitive report and uses the same methodology.

To determine the extent to which efforts to transform the physical security program at NIST incorporated key practices and addressed security vulnerabilities, we reviewed documentation and testimonial evidence associated with actions that NIST and Commerce management have taken and compared this information to selected key practices for successful organizational transformations.⁷ In addition to interviewing Commerce and NIST management, we interviewed PSG officers and contract guards at the Gaithersburg and Boulder campuses to identify challenges that may affect the implementation of physical security policies and procedures. To identify common themes related to the perspectives of NIST scientific and technical employees about NIST’s physical security program, we conducted a generalizable survey of 506 randomly selected NIST employees from six of NIST’s Laboratory Programs, which represent 84 percent of NIST’s nonmanagement, scientific and technical

⁶GAO, *Physical Security: NIST and Commerce Need to Complete Efforts to Address Persistent Challenges*, [GAO-18-14SU](#) (Washington, D.C.: Oct. 4, 2017).

⁷We have previously identified key practices of successful large-scale organizational transformations. Because NIST identified the need to transform its security culture as an agency-wide effort, we determined it was appropriate to assess NIST against five of these key practices, specifically: (1) top leadership drives the transformation; (2) establish a coherent mission and integrated strategic goals to guide the transformation; (3) focus on a key set of principles and priorities; (4) set implementation goals and a timeline; and (5) establish a communication strategy to create shared expectations and report related progress. For the purposes of this report, 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).

personnel.⁸ The survey included federal NIST employees, as well as NIST associates, who may be guest researchers, students, or contractors. All percentage estimates from the survey questions are generalizable to the overall population with confidence intervals (a measure of sampling error) no wider than ± 7 percentage points at the 95 percent level of confidence, unless otherwise noted. See appendix I for a detailed discussion of our survey methodology.

In addition, we conducted covert surveillance and nongeneralizable vulnerability testing to determine the extent to which NIST and OSY personnel abide by security policies and procedures and to identify any challenges that exist with regard to securing both NIST campuses. This testing used in-person scripted and predetermined scenarios at selected buildings and facilities at the Gaithersburg and Boulder campuses. All covert vulnerability testing activities were conducted by GAO agents during normal business hours on consecutive days. The results of our vulnerability testing are illustrative, and cannot be generalized.

To determine the extent to which the organizational structure of the NIST security program reflects best practices, we reviewed available information to develop a comprehensive description of the organizational structure of the physical security program at NIST. This information included policies, procedures, information related to NIST's law-enforcement delegation of authority, and NIST's service-level agreement with OSY. We also reviewed incident data from fiscal year 2015 through the second quarter of fiscal year 2017 to better understand the types of security incidents NIST law enforcement responded to during that time.⁹ In addition, we interviewed senior officials at NIST and OSY who play a policy, supervisory, or operational role in NIST's physical security program. We assessed this information against the ISC's Best Practices for Planning and Managing Physical Security Resources.¹⁰

⁸There were 626 scientific and technical personnel from NIST's Information Technology Laboratory and two staff offices inadvertently excluded from our target population. Subsequent analysis showed that their exclusion did not affect our conclusions.

⁹We assessed the reliability of these data by interviewing knowledgeable officials and electronically testing for missing data, outliers, and errors. We found these data to be reliable for our purposes.

¹⁰Interagency Security Committee, *Best Practices for Planning and Managing Physical Security Resources: An Interagency Security Committee Guide* (December 2015).

To determine the extent to which NIST's risk management process incorporates ISC standards and best practices, we compared OSY and NIST's risk management activities performed for both campuses to the RMP Standard. For our analyses, we compared NIST and OSY's risk management activities to versions of the RMP Standard that were applicable at the time each given activity took place.¹¹ Given that the most-recent risk assessments conducted by OSY and NIST were dated 2015 and 2017, respectively, we focused on risk management activities performed during those time frames, as well as any plans for future policy changes. We compared OSY's department-wide security manual, its 2015 assessment reports, and NIST's formal responses to those reports to the 2013 version of the RMP Standard. We then compared documentation of NIST's 2017 risk assessment and decision-making processes to the 2016 version of the RMP Standard. Further, we interviewed OSY, NIST, and ISC officials to determine the extent to which policies under development during our review would incorporate the RMP Standard. We also interviewed officials and reviewed documentation from Commerce's National Telecommunications and Information Administration (NTIA) and National Oceanic and Atmospheric Administration (NOAA) to determine the extent of their roles in NIST's risk management activities for the Boulder campus, where they are tenants.

We conducted this performance audit from August 2016 to October 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. We conducted our related investigative work from September 2016 to March 2017 in accordance with investigative standards prescribed by the Council of the Inspectors General on Integrity and Efficiency.

Background

NIST Mission and Organizational Structure

NIST serves as the federal government's focal point for conducting scientific research and developing measurements, standards, and related

¹¹The ISC periodically updates the RMP Standard and its appendixes.

technologies. NIST activities span seven laboratory programs under the Associate Director for Laboratory Programs that cover a wide range of subject matter, such as bioscience and health, energy, manufacturing, and public safety and security.¹² Additionally, there are six management support offices and four staff offices under the Associate Director for Management Resources. As of July 2017, NIST employed approximately 3,500 federal personnel and hosted 4,000 associates, who include guest researchers and collaborators, student interns, facility users, and contractors.¹³

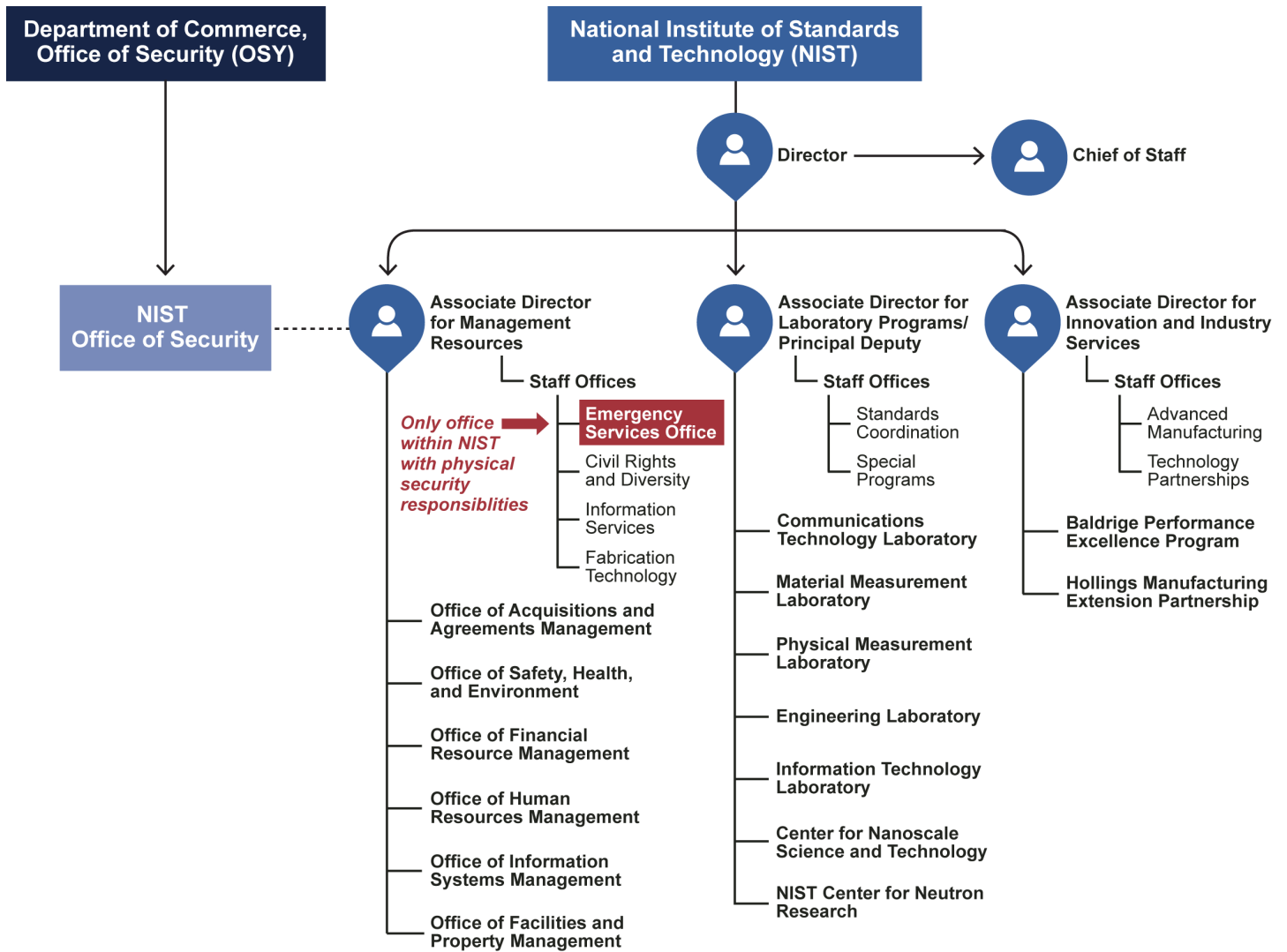
The Emergency Services Office, a staff office within Management Resources, is the only office within NIST with physical security responsibilities. All other physical security responsibilities are carried out by security personnel in the NIST Office of Security, which is located within Commerce's OSY. The PSG operates under a law-enforcement delegation of authority granted to Commerce by the Federal Protective Service (FPS).¹⁴ The delegation of authority allows the PSG to enforce federal laws and regulations, conduct investigations related to offenses against the property and persons on the property, and arrest and detain persons suspected of federal crimes on the NIST campuses. See figure 1 for the organizational chart under which NIST's physical security program operates.

¹²In addition to the seven primary laboratory programs, NIST operates extramural programs under the Associate Director for Innovation and Industry Services, including the Baldrige Performance Excellence Program and the Hollings Manufacturing Extension Partnership. NIST also has employees working in four other locations: JILA, a physics research institute formerly known as the Joint Institute for Laboratory Astrophysics; the Institute for Bioscience and Biotechnology Research; the Joint Quantum Institute; and the Hollings Marine Laboratory. Physical security for these locations is not provided by NIST, and therefore they have been excluded from our scope.

¹³We determined that approximately 4,000 employees and associates were classified as nonmanagement, scientific and technical personnel, as of December 2016. For additional information regarding how we arrived at this determination, see app. I. NIST facilities are available for use by qualified researchers from industry, academia, and government.

¹⁴FPS is a component of DHS, and is responsible, in part, for managing DHS's delegations of authority program, including determining—based on cost and capabilities analyses—whether another federal department or agency should be authorized to provide its own law enforcement or to manage its own security services at its facilities instead of FPS. Under the Homeland Security Act of 2002 (Pub. L. No. 107-296, § 1706(b)(2), 116 Stat. 2135, 2318, Nov. 25, 2002), the Secretary of Homeland Security may delegate authority for the protection of specific buildings to another federal agency where, in the Secretary's discretion, the Secretary determines it necessary for the protection of that building.

Figure 1: Organizational Chart for Managing the National Institute of Standards and Technology's Physical Security Program, July 2017



— Formal reporting requirement
 - - - - - No formal reporting requirement

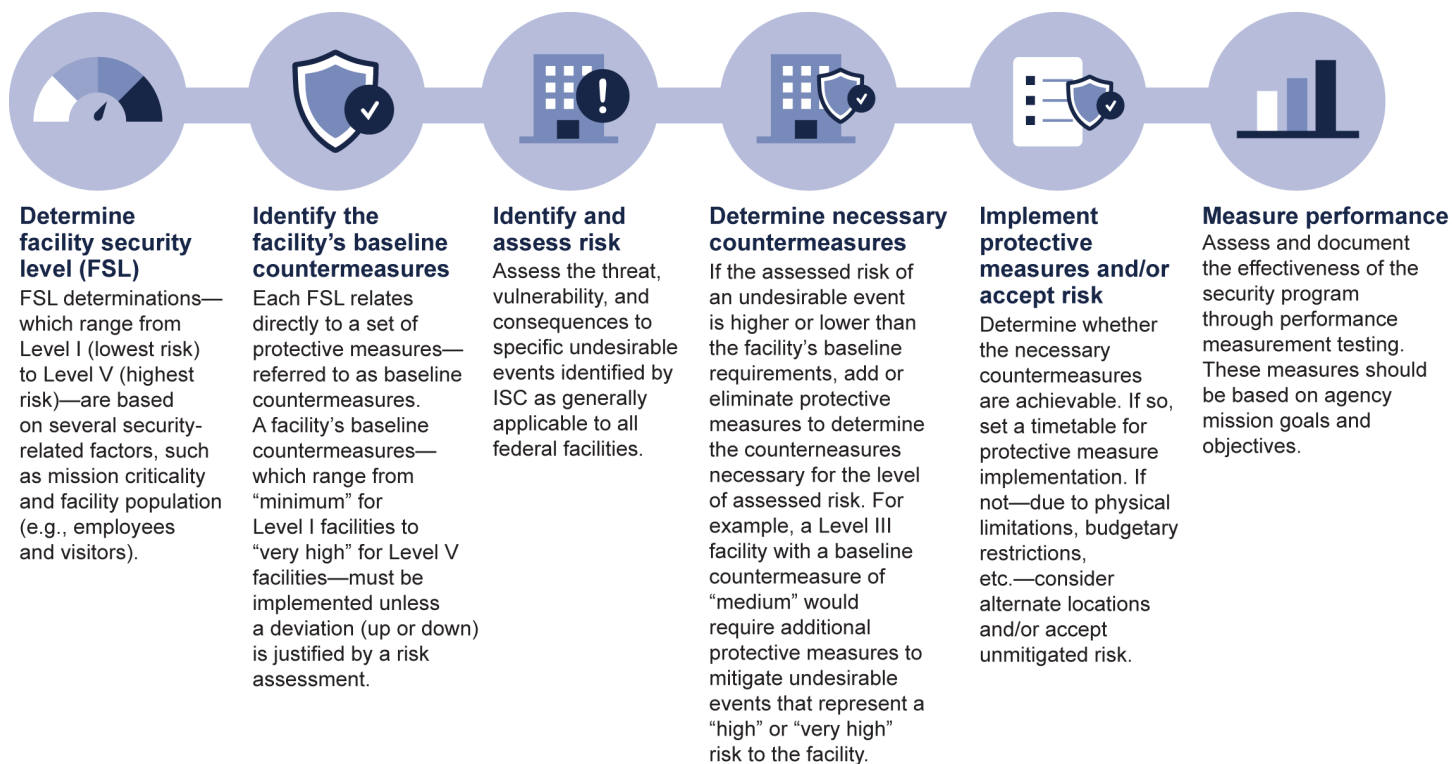
Source: Department of Commerce and NIST. | GAO-18-95

The ISC Risk Management Process

According to the ISC, risk management is a comprehensive approach to allocating resources for the protection of a facility, assets, and occupants to achieve an acceptable level of risk. Risk management decisions are

based on the application of risk assessment, risk mitigation, and, when necessary, risk acceptance. In August 2013, the ISC issued the first edition of the RMP Standard, and subsequently updated the standard in December 2016. The RMP Standard defines the criteria and processes to determine the facility security level (FSL) and provides a single source of physical security countermeasures, as well as guidance for customizing countermeasures for federal facilities. The RMP Standard requires officials responsible for the risk management process at federal facilities to follow a series of steps that are summarized in figure 2.

Figure 2: Summary of the Interagency Security Committee’s Risk Management Process



Source: GAO analysis of Interagency Security Commission information. | GAO-18-95

The FSL determination is the first step in the RMP Standard and must be performed prior to each risk assessment. FSL determinations range from Level I (lowest risk) to Level V (highest risk). The FSL is based on an analysis of six security-related facility factors, five of which are required.

The five required factors are: mission criticality, symbolism, facility population, facility size, and threat to tenant agencies.¹⁵ Assessors must evaluate and assign scores to these five FSL factors to calculate a preliminary FSL. As needed, assessors may also consider a sixth factor—the intangible factor—to adjust the FSL one level up or down based on other characteristics unique to the facility.¹⁶ Each FSL corresponds to a level of risk for the facility, which directly relates to a baseline level of protection, or the specific countermeasures required to mitigate that level of risk.

To determine whether the baseline level of protection is sufficient or customization is required, agencies must perform a risk assessment to identify and assess risks to their facilities. While the RMP Standard does not mandate the use of a specific risk assessment methodology, it requires agencies to adhere to the fundamental principles of a sound risk assessment methodology. In part, this includes the assessment of the threat, vulnerability, and consequence of specific undesirable events, such as theft, explosive devices, and active shooters.¹⁷ The RMP Standard's appendixes identify undesirable events, all of which agencies must consider as part of their risk assessment methodologies. After

¹⁵According to the RMP Standard, the mission criticality score is based on criticality of the missions carried out by federal tenants in the facility (not by the tenant agencies overall). The symbolism score is based on external appearances or well-known operations within the facility that indicate it is a U.S. government facility, as well as the potential negative psychological impact of an undesirable event occurring at the facility. The facility population score is based on the peak total number of personnel in government space, including employees, on-site contract employees, and visitors. The facility size score is based on the square footage of all federally occupied space in the facility. Lastly, the threat to tenant agencies score is based on the nature of federal tenant's contact with the public and the mission at the facility; past or current credible threats to the federal tenants at the facility (including indirect threats to federal tenants caused by threatening nonfederal tenants); and crime statistics.

¹⁶For example, the RMP Standard states that agencies may justify reducing the preliminary FSL due to factors such as a short duration of occupancy at a facility, which may reduce the value of the facility in terms of investment or mission. Agencies may justify increasing the preliminary FSL due to factors such as the potential for cascading effects or downstream impacts on interdependent infrastructure, or costs associated with the reconstitution of the facility.

¹⁷The RMP Standard defines "threat" as the intention and capability of an adversary to initiate an undesirable event; "vulnerability" as a weakness in the design or operation of a facility that an adversary can exploit; and "consequence" as the level, duration, and nature of the loss resulting from an undesirable event. It defines "undesirable event" as an incident that has an adverse impact on the facility occupants or visitors, operation of the facility, or mission of the agency.

adjusting the baseline level of protection based on this assessment, officials will determine whether the necessary level of protection is achievable, and, if not, may consider alternatives or accept the risks to the agency.

The RMP Standard also recognizes that facilities may be colocated among other federal facilities or be occupied by multiple federal tenants.¹⁸ A campus consists of two or more facilities that are located adjacent to one another and share some aspects of the environment (such as vehicle access roads or gates) or security features (such as a perimeter fence or guard force). A campus may be occupied by a single tenant, or multiple tenants. A multitenant facility consists of two or more tenants in a single facility. At multitenant facilities, the RMP Standard requires the establishment of a facility security committee (FSC) to address security issues and approve the implementation of security measures and practices. An ISC official confirmed that this also applies for multitenant campuses. The FSC consists of representatives of all tenants in the facility, the security organization, and the owning or leasing department or agency.¹⁹

¹⁸For the purposes of this report, we refer to federal facilities as “facilities” and to federal tenants as “tenants.” According to the RMP Standard, a federal facility is a government-leased or government-owned facility in the United States (inclusive of its territories) occupied by federal employees for nonmilitary activities. A federal tenant is a federal department or agency that pays rent for use of space in a federal facility.

¹⁹Appendix D within the RMP Standard outlines specific procedures for conducting an FSC, including voting procedures for tenants. For FSC voting purposes, this appendix further defines “tenant” as those listed in Appendix C of the Office of Management and Budget Circular No. A-11.

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.²⁰ In particular, leadership has taken steps to improve organizational culture associated with physical security, such as by obtaining independent security assessments and issuing an overarching Security Policy. By taking these steps soon after a significant security incident, 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. However, we found that varied levels of staff awareness about security responsibilities created security vulnerabilities. Further, NIST's ongoing efforts to address these issues do not incorporate other key practices, such as establishing a communication strategy, interim milestone dates, and measures to assess effectiveness.

NIST Leadership Has Taken Steps to Transform the Organizational Culture Related to Physical Security at NIST

NIST leadership has taken steps to transform the security program and culture at NIST since 2015. We have previously reported that at the outset of organizational transformations, it is important that leaders move quickly to "make a statement" about the importance of change, demonstrate a conviction to making it, and focus on a key set of priorities and principles. On the basis of our survey, we estimate that as of May 2017, about three-quarters of 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.²¹ Specifically, following the security incident at the Gaithersburg campus in July 2015, the NIST Director at the time requested independent security

²⁰[GAO-03-669](#). For our prior work, we convened a forum to identify useful practices and lessons learned from major private and public-sector organizational mergers, acquisitions, and transformations. Key practices we identified for effective organizational transformation include ensuring top leadership drives the transformation and establishing a communication strategy to create shared expectations and report related progress, among others.

²¹We conducted a generalizable survey from March 17, 2017, through May 10, 2017. NIST leadership includes the NIST Director (78 percent of survey respondents assessed the leader as placing great or very great importance on physical security issues), Associate Directors (73 percent), Division Director (77 percent), or Laboratory Director (75 percent). All percentage estimates from the survey questions have confidence intervals (a measure of sampling error) no wider than ± 7 percentage points at the 95 percent level of confidence, unless otherwise noted.

assessments, which were completed in December 2015. The Director subsequently developed an agency-wide Action Plan to address the assessments' findings, which was finalized in April 2016. After taking over in January 2017, the Acting Director initiated a Security Prioritization Sprint (Security Sprint), which, according to officials, built upon the transformation efforts the previous NIST Director had begun.²²

Action Plan

In response to the three independent security assessments commissioned following the July 2015 security incident, the NIST Director at the time created an Action Plan outlining key priorities for transforming the security program at NIST. This Action Plan was finalized in April 2016, and identified six themes, such as culture, organization, and risk, that needed to be addressed to improve NIST's physical security program. Within these themes, the Action Plan also identified 21 specific actions, including the need for a Security Advisory Board (SAB). Additionally, to address two of the other identified actions, NIST developed an overarching Security Policy. NIST implemented the SAB and Security Policy in 2016, demonstrating leadership's commitment to transforming NIST's security culture.²³

- **Security Advisory Board.** NIST established the SAB in September 2016. Members include senior NIST leadership, such as the Associate Director for Management Resources and the Associate Director for Laboratory Programs, as well as selected Laboratory Directors. The Director of the Emergency Services Office and the OSY Director of Security for NIST serve as co-chairs. The SAB's charter affirms the commitment of NIST management to establishing and maintaining a comprehensive, effective, and efficient agency-wide

²²According to officials, the themes of the Action Plan were also integrated into Chapter MR-10, "Security," of NIST's draft Enterprise Risk Management framework. However, according to officials, work on the MR-10 chapter has been suspended indefinitely because its findings and recommendations have been incorporated into the Security Sprint.

²³Other items from the Action Plan that NIST has implemented include establishing the NIST Director as the designated executive authority responsible and accountable for security of NIST, its facilities, staff, and assets; and disabling personal identification number access in Boulder.

approach to physical security at NIST.²⁴ The first meeting of the SAB took place in January 2017, with subsequent meetings held in April, May, June, and August 2017. SAB activities during these meetings have been consistent with the charter. For example, during the April 2017 meeting, the SAB discussed the findings of the Security Sprint.

- **Security Policy.** NIST issued its overarching Security Policy in October 2016 in support of the Director’s efforts to create security culture change at NIST. The purpose of the Security Policy is to “establish the NIST policy for ensuring the security of NIST personnel, buildings, and other plant facilities, equipment, property, and assets.” To accomplish this objective, the Security Policy identifies primary goals of NIST’s security program, such as setting and communicating clear and sustainable security objectives and employee expectations. In accordance with the key practices for organizational transformation, the Security Policy also establishes an agency-wide mission for the security program, and demonstrates leadership’s commitment to specific actions related to ensuring security. On the basis of our survey results, we estimate that 80 percent of scientific and technical employees believe that NIST is “extremely” or “very successful” at achieving the purpose of the Security Policy, while 3 percent believe that NIST is only “slightly successful.”²⁵ In addition, about 50 percent of employees reported that NIST was doing “well” or “very well” at achieving each of the specific actions included in the Security Policy. This suggests, from the perspective of employees, that NIST leadership has effectively conveyed the broad goals of the Security Policy.

Security Sprint

On February 7, 2017, the Acting NIST Director charged the NIST Chief Safety Officer (the Report Lead) with leading a Security Sprint effort. To

²⁴According to its charter, the SAB makes security-related recommendations to the NIST Director; provides input, advice, and counsel on security matters to both the Director of the Emergency Services Office and the OSY Director of Security for NIST; reviews and evaluates recommended changes to the NIST security program; and is expected to assist with the development and implementation of a long-term security management strategy; among other things. The charter states that the SAB will meet at least quarterly and may schedule additional meetings as appropriate.

²⁵Our survey questionnaire informed respondents that NIST’s Security Policy states that “It is NIST’s policy to establish and maintain a comprehensive, effective and efficient agency-wide approach to ensuring the security of NIST personnel, buildings and other plant facilities, equipment, property and assets, while maintaining a world-class laboratory-based research and development organization.” The questionnaire then asked respondents to rate how successful, if at all, NIST is at achieving the goals stated in its Security Policy.

meet the charge, the Report Lead assembled a team composed of two staff members from NIST's Enterprise Risk Management Office and consulted with subject-matter experts. According to NIST officials, the Security Sprint supersedes the Action Plan and is the latest step in NIST's leadership efforts to address the security culture. The goal of the Security Sprint was to develop a report that prioritizes security needs, their related mitigations, and actions necessary to address those needs, within NIST's activities and missions.²⁶ The Report Lead submitted the final Security Sprint report to the Acting NIST Director on March 27, 2017. The final report identified three systemic security weaknesses: (1) less than optimal organizational arrangements; (2) lack of leadership in establishing a positive security culture; and (3) significant gaps in the NIST security program.²⁷ Additionally, as discussed later in this report, the Security Sprint also assessed undesirable event risks.

The Security Sprint report identified and prioritized vulnerabilities associated with the three systemic security weaknesses and undesirable event risks, as well as the mitigations needed to address each of these vulnerabilities. For the vulnerabilities associated with the systemic security risks, the report also identified an estimated time for implementation and prioritized each as high, medium, or low. The Report Lead then created a prioritized list of actions designed to address the first half of the vulnerabilities identified. These actions include things such as: (1) establish clear baseline security requirements and roles, responsibilities, authorities, and accountabilities for the NIST staff; and (2) expand security awareness training on topics such as active shooter, workplace violence, general crime prevention measures, and suspicious packages.²⁸ According to NIST officials, following the Acting Director's approval on May 4, 2017, the Report Lead began developing detailed action plans for each of the prioritized actions, which were presented to

²⁶The Acting Director's written charge required the Report Lead to provide a product containing: (1) a rank-ordered list of security risks and threats with ranking based on potential impact to the NIST mission; (2) a prioritized list of mitigations for each risk; and (3) an estimate of cost and time to completion. The goal was to complete this effort within 30 days.

²⁷To identify these weaknesses, the Security Sprint report relied, in part, on the findings of existing security risk information, including the three independent assessments (dated December 2015), and the Action Plan developed in response to those assessments.

²⁸Other actions include (1) establish clear NIST security program requirements and roles, responsibilities, authorities, and accountabilities beyond the baseline; and (2) exercise leadership and improve accountability and understanding.

the SAB on August 2, 2017, and approved by the Acting NIST Director on August 4, 2017.

Key practices associated with successful organizational transformations include focusing on a key set of principles and priorities and setting implementation goals and timelines to provide an objective means of tracking and reporting progress. The overall Security Sprint report identifies key priorities for the agency to focus on as the transformation of the physical security program proceeds. Further, each of the action plans details the specific milestone activities needed to complete the identified action, as well as the individuals responsible for each milestone activity. The action plans provide start dates for the initial milestone activity and targeted completion dates for the final activity.²⁹ NIST officials stated that the SAB will be responsible for monitoring the implementation of the action plans against these dates; however, the plans do not contain interim milestone dates that could help assist in tracking and communicating progress of the plans' implementation. For example, one action plan identifies 10 milestone activities, providing a start date for the first activity and a targeted completion date for the last activity. Because there are no targeted dates associated with 8 of the milestone activities, NIST officials will be limited in their ability to monitor progress and make appropriate adjustments, should the timelines slip.

Efforts Do Not Fully Address Security Vulnerabilities

Although NIST leadership has taken some steps to transform the organizational culture related to physical security at NIST, these efforts do not fully address security vulnerabilities resulting, in part, from the limited effectiveness of NIST's security-related communication efforts. Our covert vulnerability testing identified security vulnerabilities. Specifically, GAO agents gained unauthorized access to various areas of both NIST campuses. The findings from our covert vulnerability testing represent illustrative examples and are not generalizable.³⁰

²⁹On the basis of the targeted completion dates, NIST expects all of the action plans to be completed by the first quarter of fiscal year 2019.

³⁰Specific details about the methodology and results from our covert vulnerability testing are sensitive and were omitted from this report.

Our survey results also identify security vulnerabilities.³¹ We asked NIST survey respondents how they would behave in several different scenarios involving certain NIST security policies. We estimate that the majority of employees would comply with security policies, though some would not, depending on the scenario presented.³² Some employees also reported that they have observed other NIST employees violating certain NIST security policies. However, 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.³³ The remainder of NIST's employees currently have no mandatory security training, and a higher percentage reported having observed a colleague not following NIST security policies.

In part to help improve the security culture at the agency, the former NIST leadership had taken some steps to improve communication with employees about security. For example, according to officials, one step NIST took to reinforce the requirement that employees display their badges while on a NIST campus was to issue a new directive on Facility Access Cards and Electronic Access Control in June 2016. In addition, several security events took place on both campuses to inform employees about recent security incidents and planned changes to the security program. For example, OSY held Security Awareness Day events at NIST in September 2015 and in 2016, and the NIST Director at the time held two campus-wide town hall meetings—in February 2016 at the Gaithersburg campus and in July 2016 at the Boulder campus.³⁴ Security Awareness Day included presentations related to insider threats and how to respond in an active shooter situation, among others. At the NIST-wide town halls, NIST leadership discussed recent security incidents, security improvements to NIST facilities, and potential changes to security systems such as installation of a fence at the Boulder campus.

³¹We 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.

³²Details related to the specific scenarios and behaviors we asked about, as well as the associated survey results, are sensitive and were omitted from this report.

³³If employees working in these facilities do not complete the training as required, access to the facilities is revoked.

³⁴OSY held previous Security Awareness Days in 2011 and 2012.

National Institute of Standards and Technology (NIST) Employee Perspective on Security Day

"I don't attend all of the talks at these events, so I can't say for sure."

Source: GAO. | GAO-18-95

Note: Open-ended response from GAO survey of NIST employees.

However, the effectiveness of these communication efforts has been limited, in part because of varied levels of staff exposure. Specifically, NIST did not require mandatory attendance at the security events held in 2015 and 2016, and does not plan to require attendance at future Security Awareness Day events. On the basis of our survey results, we estimate that 33 percent of employees have had no experience with Security Awareness Day, and 24 percent of employees have never attended NIST-wide security events. Exposure to NIST's security-related communication efforts also varies based on employee type. Specifically, our survey results show that federal employees are generally more likely than associates to attend Security Awareness Day and NIST-wide security briefings.³⁵ From February 2016 to July 2016, the NIST Director at the time also used e-mail outreach to communicate key security-related information to employees, including changes the Director planned to implement to transform the security culture at NIST, such as halting the use of personal identification number codes and new after-hours access procedures, among other things. Of the communication efforts we asked about in our survey, fewer employees had no experience with e-mail outreach than with other efforts.³⁶ On the basis of our survey results, we estimate that between 15 and 33 percent of NIST's scientific and technical employees had no experience with the security-related outreach efforts we asked about. However, the majority of employees who were exposed to the NIST security-related communication efforts found all efforts to be of at least moderate value.³⁷

³⁵According to our survey, an estimated 53 percent of federal employees attended NIST-wide security briefings and events such as Security Awareness Day once a year and about 17 percent attended more than once a year. However, an estimated 25 percent of associates attended once a year and about 21 percent attended more than once a year. Further, about 39 percent of associates reported "not at all" when asked whether they have attended NIST-wide security briefings or events, compared to 8 percent of federal staff.

³⁶When asked about the value of various communication efforts, an estimated 15 percent responded that they had no exposure to security-related e-mail outreach. For other efforts, staff reported having no experience as follows: Security Day (33 percent); NIST-wide security briefings (29 percent); other, not NIST-wide training, briefings, town hall meetings (28 percent); and other events or information on physical security (74 percent).

³⁷We asked staff how much value, if any, security events and information have been to their overall knowledge of physical security. Staff reported they found "great value" or "very great value" as follows: Security Day (32 percent); NIST-wide security briefings (31 percent); other, not NIST-wide training, briefings, town hall meetings (29 percent); and information from e-mails and other announcements (36 percent).

On the basis of the Security Sprint action plans introduced in August 2017, NIST intends to continue to rely on Security Awareness Day and all-staff meetings to provide ongoing security communications, though the agency will not require mandatory attendance at these events. In addition, however, the action plans indicate that NIST intends to implement two types of required security training. First, after developing new security baseline requirements, NIST will require all existing and new staff to complete a onetime training related to these requirements. According to the action plan, this onetime requirement is intended to address the need for an effective communication plan identified by the Security Sprint report. Similarly, for another action, NIST will require staff to complete active shooter training.

Developing a communication strategy to create shared expectations and monitor progress is another key practice for successful organizational transformations.³⁸ Communication is most effective when done early, clearly, and often, and a communication strategy should seek and monitor employee attitudes and take appropriate follow-up action. For example, obtaining employees attitudes at the outset of the transformation through mechanisms such as surveys can serve as a measurement of how effective is leadership at executing the organizational change. However, the action plans do not include activities associated with measuring whether security-related information is effectively being communicated to staff. These mandatory training requirements, if implemented as intended, could help improve the effectiveness of leadership's efforts to communicate security-related information. However, without establishing a broader communication strategy, including measures to assess the effectiveness of these efforts, it remains unclear whether they will mitigate any of the security vulnerabilities we identified.

Despite the efforts by the former NIST Director to improve communication with employees about security, the Security Sprint found that there was no consistent, clear message provided to NIST employees regarding their role in security and basic expectations that employees were expected to meet. For example, the Facility Access Cards and Electronic Access Control directive details staff requirements associated with access controls and badging. According to the Security Sprint Report Lead, however, the directive does not provide employees with an understanding of expected behaviors associated with carrying out the requirement. To

³⁸[GAO-03-669](#).

address these security vulnerabilities, the Security Sprint report recommended that NIST develop and implement an effective communication plan. Officials told us the action plans will address this concern by developing detailed behavioral expectations for employees related to security requirements and responsibilities and incorporating them into a revised security policy. However, the action plans NIST released did not include requirements specifically associated with behaviors, and did not identify how these requirements might fit into a broader communication strategy.³⁹

National Institute of Standards and Technology (NIST) Employee Perspective on Security Culture

"[I]f you want to strengthen the physical security culture at NIST, you have to help the people here understand why this is important."

Source: GAO. | GAO-18-95

Note: Open-ended response from GAO survey of NIST employees.

As we have previously reported, effective communication strategies, clear implementation goals and time frames, and monitoring progress are essential to successfully transforming organizational culture.⁴⁰ According to officials, NIST intends to use periodic security-culture surveys as one way to monitor progress and measure effectiveness, but the Security Sprint action plans introduced in August 2017 did not include conducting a survey or any other activities to measure the plans' effectiveness. Further, the targeted completion dates included in the action plans are provided only for the final activity in each plan, limiting NIST's ability to track progress of the interim activities. By incorporating elements of key practices, including a comprehensive communication strategy, interim milestone dates, and measures to assess the effectiveness of the action plans, NIST will be better positioned to effectively address the security vulnerabilities caused by varied levels of security awareness among employees.

³⁹Although the baseline behavioral requirements have not been developed, officials provided us with several illustrative examples of the type of guidance they intend to provide employees. These details are sensitive and were omitted from this report.

⁴⁰[GAO-03-669](#).

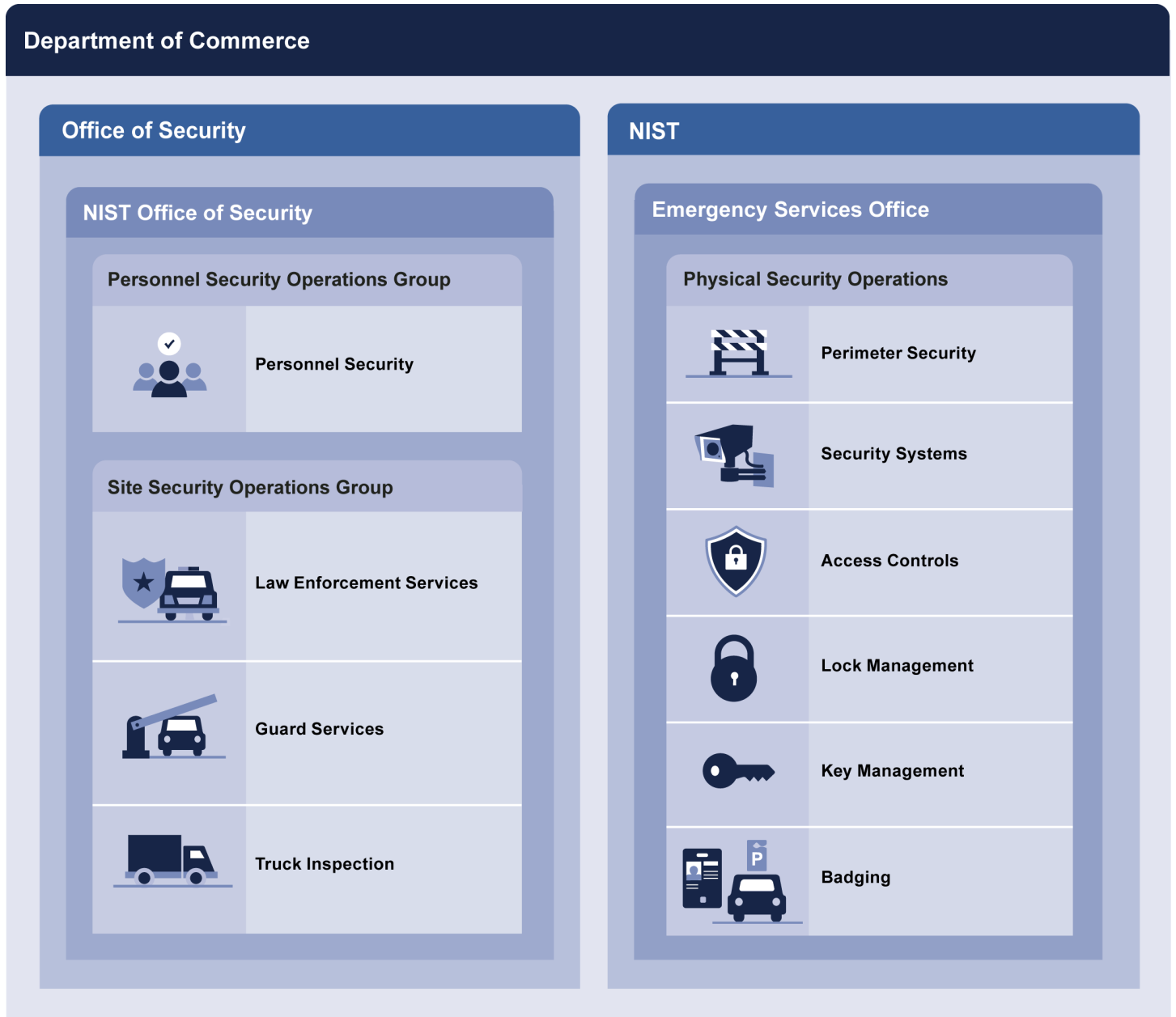
The Organizational Structure of NIST's Physical Security Program Does Not Fully Reflect Best Practices, Potentially Inhibiting Effectiveness

The organizational structure of NIST's physical security program is fragmented and does not fully reflect best practices. We found that neither OSY nor NIST has assessed, or plans to assess, whether the current structure is the most appropriate way to fulfill NIST's security requirements, despite related findings within the Action Plan and Security Sprint. As a result, the structure, which has been in place since October 2015, is likely creating unnecessary inefficiencies and competing priorities, thereby inhibiting the effectiveness of the physical security program overall, as well as ongoing efforts to improve the program.

Specifically, inconsistent with best practices, responsibility for physical security is split between OSY and NIST, and management of the program is fragmented.⁴¹ OSY operates NIST's Office of Security, which is responsible for managing law-enforcement services (the PSG), contract-guard services, and personnel security, which includes suitability, screening, and security clearances for employees, foreign nationals, and contractors. NIST's Emergency Services Office is responsible for the physical security infrastructure, such as access control technology and perimeter security infrastructure. See figure 3 for additional detail about how security responsibilities are distributed.

⁴¹We 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).

Figure 3: Physical Security Responsibilities at the National Institute of Standards and Technology (NIST), as of July 2017

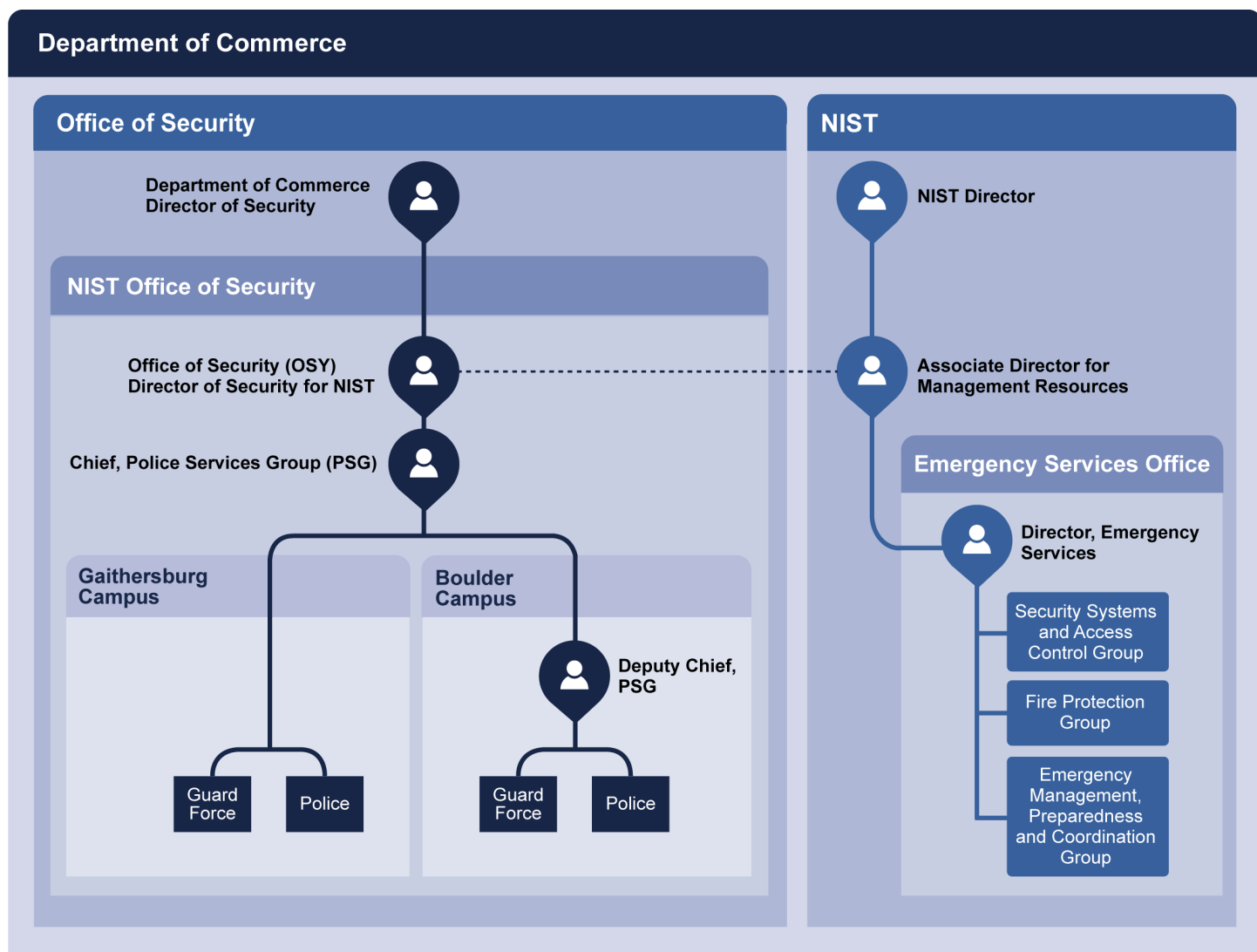


Source: Department of Commerce and NIST. | GAO-18-95

Many of OSY and NIST’s responsibilities 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. However, management and oversight of physical security activities is fragmented. Specifically, the head of NIST’s Office of Security—the OSY Director of Security for NIST—reports to the OSY Director of Security within Commerce, while the Director of the Emergency Services Office reports to the NIST Associate Director for Management Resources. See figure 4.

Figure 4: Management Structure of the National Institute of Standards and Technology (NIST) Physical Security Program, as of July 2017



Source: Department of Commerce and NIST. | GAO-18-95

Documented procedures for how OSY and NIST are expected to coordinate are inconsistent. The service-level agreement between OSY and NIST, dated October 2015, details the management and oversight responsibilities for NIST's physical security program, and seeks to ensure a minimum level of communication between OSY and NIST. For example, the agreement specifies periodic communication between OSY and NIST officials and requires that OSY provide NIST with an opportunity to review and comment on any changes to security procedures or practices within OSY's areas of responsibility.⁴² However, it does not include the same requirement for OSY to comment on changes that NIST seeks to make within its areas of responsibility. According to an OSY official, this has resulted in flaws in NIST's physical security program. For example, because OSY has no responsibility or authority regarding security technology, it cannot develop policies and procedures associated with the technology even though OSY personnel are the ones using the technology. As a result, there are no written procedures for the dispatch center, so, according to an OSY official, security personnel depend on on-the-job training to learn what to do.⁴³ Similarly, PSG officers we spoke with stated that they are not consulted about their recommendations related to security technology they use on a daily basis.

As mentioned earlier in this report, officials told us that the Security Sprint is the latest step in an iterative process and is intended to build upon the 2016 Action Plan. However, while the 2016 Action Plan clearly states that the current structure limits the effectiveness of NIST's security program, the issue is prioritized last out of the vulnerabilities identified in the

⁴²The service-level agreement specifies that the OSY Director of Security for NIST will meet at least monthly with the NIST Liaison (identified as the NIST Associate Director for Management Resources) to discuss any issues or concerns. Similarly, it specifies that the OSY Director of Security, the NIST Associate Director for Management Resources, the OSY Director of Security for NIST, and the NIST Liaison should meet semiannually to discuss the status of services. According to NIST officials, meetings have occurred more frequently. As of August 2017, the Associate Director for Management Resources, his Deputy, the Director of Emergency Services, and the OSY Director of Security for NIST met weekly to discuss NIST's security program.

⁴³According to NIST officials, OSY has notified them regarding concerns related to the dispatch center. In response, NIST officials are planning to develop a list of prioritized actions to address the identified problems by September 2017.

Security Sprint.⁴⁴ The final Security Sprint report concluded that the only option to address the structural problems would be to seek legislative change to remove OSY from management of law enforcement and site security at NIST.⁴⁵ However, according to officials in June 2017, NIST has not sought, and is not seeking, any change, legislative or otherwise, to move police and guard services from OSY to NIST or to create a single security entity fully located within NIST. The Security Sprint report also does not address the possible effect that the existing organizational challenges may have on the implementation of all of the other prioritized items. Further, while the Security Sprint requires a review of the pros and cons of “all plausible organizational arrangements and structures,” officials explained that this review will only address the possibility of combining NIST’s existing security and safety organizations. It will not address the split in management of physical security between NIST and OSY, which is a missed opportunity for NIST to thoroughly reevaluate the fragmented management structure.

The Security Sprint effort itself also exemplifies the problems that arise from fragmented program management. The Security Sprint explicitly excludes from its scope any assessment of security responsibilities that are currently assigned to OSY, despite the integral role of these responsibilities in securing the NIST campuses. Additionally, with the exception of the Security Sprint’s assessment of undesirable events (discussed later in this report), the OSY Director of Security for NIST and other security specialists within the NIST Office of Security were not involved in the Security Sprint process.

Opportunities may exist to improve implementation of NIST’s physical security program by modifying the organizational structure. OSY and NIST’s fragmented organizational structure does not fully align with the ISC’s Best Practices for Planning and Managing Physical Security Resources. These best practices encourage agencies to centrally manage physical security through a Director of Security or Chief Security

⁴⁴The independent assessments that informed the 2016 Action Plan all discussed concerns with the existing organizational structure and recommended some form of a consolidated security program. However, in some cases, the assessments also included responsibilities beyond physical security within their recommendations, such as emergency services or safety activities.

⁴⁵The American Innovation and Competitiveness Act, Pub. L. No. 114-329, § 113, 130 Stat. 2969 (Jan. 6, 2017), requires that OSY directly manage the law-enforcement and site-security programs of NIST through an assigned Director of Security for NIST.

Officer with agency-wide responsibilities for developing and implementing the agency's physical security vision, strategy, programs, and related matters. This role includes responsibility for managing and allocating physical security resources based on the agency's decisions made from risk assessments. While the best practices also 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.⁴⁶ However, it does not otherwise mandate, assign, or restrict the organizational structure and assigned responsibilities for other aspects of NIST's security program. For example, the law does not preclude OSY from taking over responsibility for physical security countermeasures at NIST. As of August 2017, NIST has not identified a Chief Security Officer, and the OSY Director of Security for NIST does not centrally manage NIST's security program, or have responsibility for a significant number of security activities.

Although the best practices acknowledge that the central management of physical security functions may not be feasible at some agencies due to various factors, we found that neither NIST nor OSY evaluated the feasibility of other organizational options for NIST's physical security program before proposing to implement the current fragmented management structure. The current management structure was established in an effort to prevent FPS from rescinding NIST's law-enforcement delegation of authority following concerns with the oversight of security personnel.⁴⁷ According to the former NIST Director involved with the process, the intention was that OSY would eventually oversee all physical security activities at NIST.⁴⁸ According to current NIST officials,

⁴⁶Pub. L. No. 114-329, § 113, 130 Stat. 2969 (Jan. 6, 2017).

⁴⁷The development of the current organizational structure began in 2010 when FPS informed NIST it would be rescinding the existing delegation of authority and taking over security and protection services at NIST. After 3 years of interim extensions of the delegation of authority, FPS granted a 5-year delegation of authority in 2013, on the condition of Commerce's ongoing implementation of changes to the operations and oversight of the PSG, among other requirements. Although NIST received a delegation of authority for both law enforcement and contract guard services, according to FPS officials, inclusion of the contract guard authority was an oversight. NIST is not required to obtain contracting authority through FPS because—with the exception of the NOAA building on the Boulder campus—the NIST campuses are not owned by the General Services Administration (GSA).

⁴⁸According to former OSY and NIST officials involved in the process, at the time, OSY did not have the capacity to immediately take over the entire program.

the agency no longer has a goal of creating a single security entity fully located in NIST, and NIST officials believe that transferring all security services to OSY would undermine the efforts of NIST leadership to improve the agency's security culture.

The Security Sprint recognized the contribution of the fragmented management structure to NIST's systemic security weaknesses, but 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 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.

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.⁴⁹ 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, which could address some issues with OSY and NIST's recent efforts. However, the two entities did not coordinate their overlapping risk management activities, which could lead to duplicative efforts, hinder potential progress toward improving NIST's physical security program, and expose the campuses to risks.⁵⁰

OSY and NIST Took Risk Management Steps in Recent Years That Did Not Fully Align with ISC Standards

OSY and NIST performed risk management steps in recent years for NIST's Gaithersburg and Boulder campuses, but did not fully align their efforts with the RMP Standard. In 2015, OSY calculated the facility security levels (FSL), performed risk assessments, and recommended countermeasures for the campuses, after which NIST decided to implement certain countermeasures. However, neither OSY nor NIST used sound risk assessment methodologies, fully documented key risk management decisions, or appropriately involved stakeholders in accordance with the RMP Standard. Further, the officials responsible for performing these risk management steps were not trained on the RMP Standard, as recommended by the Interagency Security Committee (ISC).

Risk Assessment Methodology

The RMP Standard requires agencies to use a sound risk assessment methodology, which must in part assess the threat, consequence, and

⁴⁹OSY 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 the 2015 risk management activities against the ISC's 2013 RMP Standard, and NIST's 2017 risk management activities against the 2016 RMP Standard. According to OSY, its next risk assessments for both NIST campuses will take place during fiscal year 2018.

⁵⁰[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 provided the same services to the same beneficiaries.

vulnerability for all undesirable events identified by the ISC.⁵¹ In the 2015 risk assessment reports for both NIST campuses, OSY documented its consideration of the threat, consequence, and vulnerability for certain types of undesirable events, in accordance with Commerce policy in place at the time. The RMP Standard's appendixes list the undesirable events that agencies must consider as part of their risk assessment methodologies.⁵² During the 2015 risk assessments for Gaithersburg and Boulder, there were 30 undesirable events listed in the RMP Standard. In accordance with Commerce policy, OSY did not consider most of the required undesirable events and did consider some events not listed in the RMP Standard.⁵³

We have previously reported that agencies could face deleterious effects when they do not use risk assessment methodologies that fully align with the RMP Standard.⁵⁴ By not performing sound risk assessments in 2015, OSY reduced NIST's ability to mitigate the risk of undesirable events. For example, OSY did not specifically consider undesirable events related to unauthorized access that later occurred on the NIST campuses. For example, in April 2016, an individual successfully gained unauthorized access to a secure building.

As part of its Security Sprint initiated in February 2017, NIST also independently developed and performed risk assessments for Boulder and Gaithersburg.⁵⁵ The Security Sprint team considered the threat,

⁵¹The RMP Standard defines "threat" as the intention and capability of an adversary to initiate an undesirable event; "vulnerability" as a weakness in the design or operation of a facility that an adversary can exploit; and "consequence" as the level, duration, and nature of the loss resulting from an undesirable event.

⁵²According to an ISC official, agencies are required to consider all of the undesirable events identified in the most current version of the RMP Standard's appendixes. However, this does not preclude agencies from considering other undesirable events in addition to those listed. Specific details about the undesirable events identified by the RMP Standard are sensitive and were omitted from this report.

⁵³The ISC reviews and updates its products, including appendixes, on a regular basis, including appendixes to the RMP Standard. Among other changes, updates to the appendixes may include the addition or removal of undesirable events.

⁵⁴GAO, *Facility Security: Agencies Should Improve Methods for Assessing and Monitoring Risk*, GAO-17-605SU (Washington, D.C.: Aug. 9, 2017).

⁵⁵NIST independently developed its risk assessment methodology and involved OSY in assessing the risks for both campuses on a limited basis. For example, OSY was involved with an initial step of assigning risk values to undesirable events, and then NIST adjusted and finalized those values without involving OSY.

Documentation of Key Risk Management Decisions

vulnerability, and consequence for more undesirable events than OSY did in 2015, but did not consider all of the undesirable events required by the RMP Standard at that time. According to NIST officials, NIST plans to formalize its internal risk assessment process and perform additional independent risk assessments in the future. Without finalizing and implementing policies that require consideration of all required undesirable events, NIST does not have assurance that future independent risk assessments will align with the RMP Standard.

Neither OSY nor NIST fully documented key risk management decisions during risk management steps performed for NIST's Gaithersburg and Boulder campuses in 2015 or 2017, partly because neither organization required such documentation in their internal policies. The RMP Standard states that decisions made during the risk management process must be thoroughly documented. However, OSY and NIST did not fully document decisions related to FSL determinations, and NIST did not fully document decisions about countermeasures. Absent clear documentation of key risk management decisions, OSY and NIST might be limited in having full information to make informed physical security decisions.

FSL Determinations

According to the RMP Standard, the FSL should be reviewed and adjusted, if necessary, as part of each initial and recurring risk assessment. While OSY calculated the FSLs for both campuses as part of the risk management steps performed in 2015, it did not fully document key decisions associated with its calculations. For Gaithersburg, the risk assessment report included information to justify scores for four of the five required FSL factors, but did not provide justification for the score assigned to the symbolism factor. For Boulder, the report included information to justify scores for three of the five required factors, but did not (1) justify the score for symbolism, or (2) indicate the score for threat to tenant agencies.⁵⁶ Although this level of documentation met Commerce's department-wide policy requirements, it did not meet the RMP Standard. See figure 5 for a summary of the extent to which OSY documented scores and justifications for each FSL factor in the 2015 risk assessment reports.

⁵⁶According to OSY officials, the risk assessment reports for both campuses constitute the sole documentation to justify calculations for the 2015 FSL determinations.

Figure 5: Summary of the Department of Commerce’s Documentation of Key Decisions Related to Facility Security Level (FSL) Determinations for National Institute of Standards and Technology Campuses in 2015

| FSL Factor | Gaithersburg Campus | | Boulder Campus | |
|-----------------------------|---------------------|---------------------------|-------------------|---------------------------|
| | Documented score? | Documented justification? | Documented score? | Documented justification? |
| Required | | | | |
| ▶ Mission criticality | ● | ● | ● | ● |
| ▶ Symbolism | ● | ○ | ● | ○ |
| ▶ Facility population | ● | ● | ● | ● |
| ▶ Facility size | ● | ● | ● | ● |
| ▶ Threat to tenant agencies | ● | ● | ○ | ○ |
| Optional^a | | | | |
| ▶ Intangible adjustment | Not adjusted | NA | Adjusted | ● |

- Yes
- No
- NA Not applicable

Source: GAO analysis of Department of Commerce documents. | GAO-18-95

^aThe Interagency Security Committee’s standard on the risk management process gives assessors the option to adjust the FSL up or down by one level for an intangible adjustment. However, documentation of an intangible adjustment is not optional.

Further, during the risk management steps carried out as part of the Security Sprint, NIST did not fully align with the RMP Standard with regard to FSL determinations. Specifically, NIST did not reassess the FSL for the campus in Gaithersburg as part of the Security Sprint, and instead relied on the FSL determination from 2015. For Boulder, NIST relied on an FSL change that occurred for the campus in January 2017. However, neither NIST nor OSY reviewed the five FSL factors required by the RMP Standard. Rather, according to an OSY official, they carried over Boulder’s FSL calculations from 2015 for those five factors, without reassessing them. Specifically, the official said that they just removed the intangible factor (the optional factor) from the FSL calculations. NIST and OSY documented Boulder’s FSL change in a memorandum.

According to NIST and OSY officials, NIST changed Boulder's FSL based on OSY's recommendation in 2017 after changes were made to assets on the campus. However, in Boulder's 2015 risk assessment report, the assessor's explanation for adjusting the final FSL was unrelated to those assets and no additional information was provided. The assessor retired from the department in December 2016. Because the documentation within the 2015 report was limited, OSY officials could not confirm whether the assets had contributed to the 2015 adjustment. As a result, OSY and NIST may have changed Boulder's FSL without addressing the actual issues considered by the assessor in 2015.

According to an ISC official, documentation provides longevity through access to historical information about security decisions in the event that knowledgeable officials are no longer available. Despite the RMP Standard's requirement to do so, the Commerce policy that has been in place since 2012 does not require assessors to document the support for decisions made in past risk assessment reports, such as support for FSL calculations described above. Given the transformation of the physical security program at NIST, including turnover among personnel involved, it is important to document key decisions in accordance with the RMP Standard to help ensure that officials have clear and accurate information on which to base future decisions.

Risk Acceptance and Consideration of Alternative Countermeasures

In the final steps of the ISC's risk management process, decision makers such as NIST must decide to either implement countermeasures in response to risk assessment findings, or to accept risks associated with not implementing countermeasures. The RMP Standard defines risk acceptance as the explicit or implicit decision not to take an action that would affect all or part of a particular risk. In instances when decision makers determine that the countermeasures necessary to fully mitigate risks cannot be implemented, documentation must clearly reflect the reason why implementation cannot occur. Further, when accepting risk by not implementing necessary countermeasures, decision makers must identify and document the highest achievable level of protection, or alternative countermeasures, that could partially mitigate risks.

In response to OSY's 2015 risk assessment reports, NIST did not fully document decisions regarding OSY's recommendations, partly because it was not required by Commerce or NIST policy. Specifically, neither Commerce nor NIST policy required decision makers to document (1) the reasons why certain recommended countermeasures were not

implemented at the time or (2) that alternative countermeasures were considered in those instances in accordance with the RMP Standard. Given the ongoing transformation of NIST's physical security program, the limited documentation available about decisions made in 2015 has positioned future decision makers to be less informed about potential opportunities to improve security.

In 2017, NIST's Security Sprint team eliminated certain countermeasures from consideration in its Security Sprint report for various reasons. For example, the team found that some countermeasures were of low priority. However, the Acting NIST Director (who served as the decision maker for both campuses) did not formally document approval of those decisions. NIST policy at the time did not require such documentation, but without integrating risk acceptance documentation into the risk management policy under development, NIST will limit its ability to make fully informed decisions in the future with knowledge of all past unmitigated risks.

Stakeholder Involvement in the Risk Management Process

During the risk management process at NIST in 2015, OSY and NIST made some physical security decisions without involving required stakeholders. According to the RMP Standard, all tenants who pay rent to occupy space in a facility are afforded a vote on the final FSL determination and decisions about all recommended countermeasures, which an ISC official said also applies to multitenant campuses. However, OSY made FSL calculations for both campuses, and the tenant agencies did not document agreement with the final FSL determinations. Additionally, in Boulder, NTIA and NOAA lacked decision-making authority over the countermeasures recommended by OSY. Similarly, NIST did not involve or provide decision-making authority to NTIA and NOAA during its 2017 Security Sprint.

According to the RMP Standard, the decision about the final FSL determination rests with the tenant, including instances where there are multiple tenant agencies. In Gaithersburg, a single-tenant campus, NIST did not document its approval of the final FSL determination in 2015. For multitenant campuses such as Boulder, the RMP Standard allows tenants to determine an FSL for each individual facility or an overall FSL for the entire campus, and the latter must reflect the highest security ratings among the tenants.⁵⁷ Specifically, to calculate an overall FSL for a multitenant campus, the highest rating among the tenants must be used

⁵⁷At a campus housing a single tenant, an overall FSL may be established.

to rate each FSL factor. However, according to officials, security ratings unique to NTIA and NOAA have not been considered in OSY's FSL calculations for Boulder since at least 2015.⁵⁸ Further, NIST did not provide decision-making authority to other tenant agencies when determining the FSL in Boulder. We found the following:

- NIST did not provide NTIA and NOAA with authority over the 2015 FSL determination.
- NIST and OSY coordinated to change the Boulder campus's FSL in 2017 based on changes to assets on the campus, but NIST did not give NTIA or NOAA authority in that decision-making process.

NIST also did not always provide required stakeholders with decision-making authority for responding to recommendations from OSY's 2015 risk assessments. As with FSL determinations, the RMP Standard states that decisions about implementing countermeasures rest with the tenant, which may consist of multiple agencies. However, NIST served as the sole decision maker for both campuses in 2015, and NTIA and NOAA did not have authority over decisions about OSY's recommendations for Boulder. Specifically, NIST's Chief Facilities Management Officer from the Office of Facilities and Property Management formally responded to OSY's recommendations and decided to implement certain countermeasures. Similarly in 2017, NIST did not involve NTIA and NOAA in its Security Sprint or consider the unique risks they may have. As a result, these potential risks were not reflected in the risk assessment for that campus, potentially limiting the usefulness of the assessment's findings.

Further, the RMP Standard states that multitenant facilities must establish a formal decision-making body known as a facility security committee (FSC), which an ISC official said also applies to multitenant campuses.⁵⁹ OSY and NIST agree that Boulder is a multitenant campus and that NTIA and NOAA should have decision-making authority. However, as of July 2017, neither NIST nor OSY policy required the establishment of an FSC on the NIST campus in Boulder, and as a result that campus does not currently have an FSC. Instead, the Boulder campus has a Board of

⁵⁸The GSA owns the NOAA building on the Boulder campus, and FPS provides security for that building.

⁵⁹In single-tenant facilities and campuses, such as the Gaithersburg campus, the federal department or agency with funding authority is the decision maker for the facility's security and is not required by the RMP Standard to establish an FSC.

Directors, which OSY identified as the FSC in its 2015 risk assessment report. However, the board does not fully meet the ISC's FSC requirements. The RMP Standard requires that FSC members be granted authority over security-related decisions, such as the final FSL determination. NIST, NTIA, and NOAA have members on the board, and, according to officials, security issues are sometimes discussed. While OSY and NIST officials believe NTIA and NOAA should have weighted voting rights in accordance with the RMP Standard, the board charter does not specifically grant NTIA and NOAA decision-making authority over security matters, and board members said they have not had such authority. For example, aside from being briefed on the findings from the risk assessment report, the NTIA and NOAA board members did not have authority over the campus FSL determination or decisions about countermeasures. This contrasts with the specific FSC requirements in the RMP Standard, which state that all tenants who pay rent to occupy space on a campus are afforded a vote on the final FSL determination and decisions about all recommended countermeasures.

According to an OSY official, the revised risk management policy will include requirements for establishing an FSC for multitenant campuses. However, the draft policy OSY provided in July 2017 did not contain any requirements associated with establishing an FSC. Without a policy requiring NIST to establish an FSC for Boulder, NIST will be limited in its ability to minimize risk to the people and assets on the campus by ensuring that physical security decisions are fully informed by the needs and resources of all tenant agencies. Further, without involvement from the other tenant agencies in Boulder, NIST's physical security decisions were made without complete information about risks and available resources. For example, the RMP Standard indicates that FSC members are expected to pay their prorated share of the cost of implementing countermeasures. Thus, NIST, NTIA, and NOAA may be able to jointly fund countermeasures for the campus.

Training on the RMP Standard

Neither OSY nor NIST met the ISC's requirements or best practices for risk management training during the risk management processes undertaken in 2015 and 2017. The RMP Standard requires decision makers at multitenant facilities—or FSC members—to successfully complete ISC risk management training courses.⁶⁰ According to an ISC

⁶⁰Federal employees selected to be members of a federal FSC are required to successfully complete a training course that meets the minimum standard of training established by the ISC.

official, this requirement would also apply to multitenant campuses. Further, the ISC offers free online training courses on the RMP Standard and encourages all parties involved in the risk management process (such as decision makers for single-tenant facilities and campuses and assessors) to complete that training.⁶¹ However, OSY and NIST officials involved in NIST risk management activities were not required to complete training, because it was not reflected in Commerce or NIST policy. For the risk management process in 2015, OSY assessors were not trained on the RMP Standard, which an OSY official said contributed to a lack of understanding about ISC requirements.⁶² Similarly, according to officials, in 2017 the Security Sprint team was not trained on the RMP Standard, yet performed risk management steps for NIST's campuses. By requiring training for OSY and NIST officials involved in risk management activities for NIST's campuses (including assessors and decision makers), NIST would be better positioned to make optimal physical security decisions based on the effective completion of the ISC's risk management steps.

Draft Commerce Policy Seeks to Better Align Risk Management Processes with ISC Standards

OSY's draft revisions to Commerce's department-wide risk management policy seek to better align NIST's risk management process with ISC standards. Neither OSY nor NIST had policies in place that fully aligned with the RMP Standard when they performed past risk management steps for NIST's Boulder and Gaithersburg campuses. Specifically, OSY relied on the existing Commerce policy in 2015 to perform risk management steps for the Gaithersburg and Boulder campuses, whereas NIST developed a process based partly on its safety risk management practices to independently perform risk management steps during its Security Sprint in February 2017. Because these policies and practices did not fully align with the RMP Standard, OSY and NIST used risk

⁶¹The ISC developed and offers a series of free online training courses to provide federal facility security professionals, engineers, building owners, construction contractors, architects, and the general public with basic information pertaining to the ISC and its facility-security standards, processes, and practices. For a fee, officials may also take a more-collaborative course with hands-on, interactive instruction. This course is sponsored by the Office of Personnel Management and is known as the ISC RMP Training Program. According to an ISC official, in May 2017, the ISC also began offering a free instructor-led half-day course called the Risk Management Process and Facility Security Committee Training, which it is currently offering in approximately 30 cities across the United States.

⁶²In 2015, NIST's decision maker for Gaithersburg and Boulder was the Chief Facilities Management Officer, who is no longer with the agency. NIST could not confirm whether that official completed training on the RMP Standard.

assessment methodologies that were not sound, and did not fully document key risk management decisions or appropriately involve stakeholders.

OSY established a Plans, Programs, and Compliance Division in October 2015, which was staffed and began operating in February 2016. The new division was charged, in part, with revising the risk assessment chapter of the 2012 Commerce Manual of Security Policies and Procedures to better incorporate ISC requirements. According to OSY officials, the department gradually began incorporating some ISC requirements in 2008, and OSY expects full compliance with the RMP Standard when the revised policy is implemented department-wide.⁶³ Officials stated the draft policy would be submitted for management review in August 2017, but could not confirm when it would be finalized and implemented. As of July 2017, the draft policy and associated guidance require the following:

- The use of a risk assessment methodology that considers the threat, vulnerability, and consequences for required undesirable events.⁶⁴
- Better documentation of key risk management decisions, including
 - FSL determinations, such as justification for the score assigned to each FSL factor and stakeholders' signed approval of the final determination;
 - justifications for deviations from baseline levels of risk or protection; and
 - risk acceptance and consideration of alternative countermeasures.

In addition, while the draft policy provided to us in July 2017 did not contain requirements associated with the items below, an OSY official stated that the final policy would include requirements for the following:

- The establishment of an FSC at multitenant facilities and campuses.

⁶³The ISC first issued a standard on facility security determinations in 2008. ISC, *Facility Security Level Determinations for Federal Facilities* (March 2008).

⁶⁴The 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. However, the draft Facility Security Assessment template that accompanies the policy specifies that assessors consider 32 undesirable events. OSY officials stated that the final policy will require assessors to consider all undesirable events identified by the RMP standard.

- ISC training for all OSY assessors and the individuals at given agencies who are responsible for deciding to implement countermeasures and accepting risk.⁶⁵

If finalized and implemented as intended, these policy changes and guidance could directly address some of the issues we identified in the risk management activities that OSY and NIST performed in 2015 and 2017 (see table 1). According to an OSY official, OSY will officially adopt policy changes for risk assessments that it performs department-wide when the revised policy is finalized, including for the risk assessments OSY is scheduled to perform for both NIST campuses during fiscal year 2018. Finalizing and implementing this policy will help ensure that OSY addresses the weaknesses we identified in OSY and NIST’s previous risk management activities. If these policy changes are not implemented, NIST may not have a complete understanding of the risks facing its campuses, which can limit its ability to effectively protect its people and assets.

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 | <ul style="list-style-type: none"> • Commerce did not use a sound risk assessment methodology. | <ul style="list-style-type: none"> • NIST did not use a sound risk assessment methodology. | ✓ ^a |
| Documentation of key decisions | <ul style="list-style-type: none"> • Commerce did not fully document facility security level (FSL) calculations. • NIST did not fully document decisions about countermeasures. | <ul style="list-style-type: none"> • NIST did not fully document review of FSL determinations. • NIST did not fully document decisions about countermeasures. | ✓ |
| Stakeholder involvement | <ul style="list-style-type: none"> • 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. | <ul style="list-style-type: none"> • NIST did not provide other tenant agencies with decision-making authority over the FSL determination or recommended countermeasures for its campus in Boulder. | <p>✗</p> <p>As of July 2017, Commerce’s draft policy does not require agencies to establish a facility security committee at multitenant facilities or campuses.</p> |

⁶⁵The RMP Standard requires FSC members with voting rights to complete such training, but neither decision makers at single-tenant facilities and campuses nor assessors are required to complete training.

| Issue area | 2015 Risk management activities | 2017 Security Sprint | Can this issue area be addressed by planned revisions to Commerce's policy and guidance? |
|---|---|--|--|
| Interagency Security Committee (ISC) Risk Management Training | <ul style="list-style-type: none"> Commerce assessors did not complete ISC training. NIST could not confirm that its decision maker completed ISC training. | <ul style="list-style-type: none"> NIST's assessors and decision maker did not complete ISC training. | x ^b |

Source: GAO analysis of Commerce, NIST, and ISC data. | GAO-18-95

^aThe 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. 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.

^bWhile 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.

NIST and OSY Could Better Coordinate Future Risk Management Activities

Overlap between NIST and OSY's risk management activities may lead to unnecessary duplication if efforts are not coordinated. While NIST independently took steps to improve its physical security program by completing the Security Sprint for its campuses, OSY concurrently took steps to improve Commerce's compliance with the RMP Standard department-wide. However, NIST and OSY did not coordinate their efforts. For example, although OSY was developing a new risk management policy to comply with the RMP Standard, NIST did not coordinate with OSY to ensure that risk management steps taken during the Security Sprint aligned with OSY's planned improvements. As a result, NIST missed an opportunity to leverage OSY's progress toward aligning Commerce agencies' risk management processes with the RMP Standard department-wide.

Because NIST intends to continue performing risk assessments separately from OSY, officials stated that NIST plans to formalize the risk assessment process it developed and used during the initial Security Sprint effort. According to an OSY official, it is common for tenant agencies to perform their own risk assessments, which can benefit OSY assessors when they complete their assessments. Specifically, the official said tenant agencies' risk assessments can provide OSY assessors with feedback prior to starting risk assessments, and can improve the accuracy of the findings and recommendations made by OSY. While the RMP Standard states that the security organization should perform risk assessments, an ISC official explained that it does not preclude tenant agencies from performing separate risk assessments as long as the

methodology is sound. However, ISC best practices encourage coordination among the security organization, GSA, and other federal tenants to reduce any unnecessary duplication of risk assessments of facilities.⁶⁶ 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.

Conclusions

Recent security incidents at NIST's Gaithersburg and Boulder campuses highlighted vulnerabilities and raised questions about the agency's physical security program, and our work shows that such questions persist. To its credit, NIST has acknowledged its security issues, and leadership has taken steps to transform NIST's physical security program, in part by beginning to address the organizational culture, policies, and risk management at its campuses. While these efforts have met some key practices for successful organizational transformations, GAO agents were able to gain unauthorized access to various areas of both campuses. Additionally, our survey results showed that varied levels of staff awareness created security vulnerabilities. Further, the organizational structure of NIST's physical security program does not align with ISC best practices and consequently may not be the most-effective approach to physical security at NIST. By incorporating other key practices, such as implementing communication strategies and establishing interim milestone dates and measures to assess effectiveness, and by evaluating the effectiveness of different organizational structures, NIST could help ensure that the transformation of its physical security program is successful.

OSY has also taken steps to better align Commerce's risk management activities with the RMP Standard, by including these requirements in its draft policy. The revised risk management policy could improve risk management processes at Commerce department-wide, including at NIST, but NIST is in the process of developing its own risk management policy, which could lead to unnecessary duplication. Without finalizing and implementing ongoing efforts at both OSY and NIST, and coordinating with OSY to develop and implement policies, the transformation of NIST's security culture may be unsuccessful. As a result, inefficiencies and

⁶⁶ISC, *Best Practices for Planning and Managing Physical Security Resources*.

security vulnerabilities may continue to persist at the NIST campuses, putting their assets and personnel at risk.

Recommendations for Executive Action

We are making a total of four recommendations, including two to NIST and two to OSY:

The NIST Director should incorporate elements of key practices into the implementation of the Security Sprint action plans, by establishing a comprehensive communication strategy for employees; interim milestone dates; and measures to assess effectiveness. (Recommendation 1)

The Director of OSY, in coordination with the NIST Director, should conduct an evaluation of the effectiveness of the current security management structure as compared to a consolidated security structure, centrally managed by OSY, to identify the most effective and feasible approach to physical security at NIST. (Recommendation 2)

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, by requiring the following:

- Use and documentation of a sound risk assessment methodology that assesses the threats, vulnerabilities, and consequences for each of the undesirable events required by the RMP Standard, and use of these three factors to measure risk.
- Documentation of key risk management decisions, such as justification and tenants' approval for facility security level (FSL) determinations, justification for deviation from baseline levels of risk or protection, as well as risk acceptance and consideration of alternative countermeasures.
- Establishment of a facility security committee (FSC) at multitenant facilities and campuses, including locations such as the NIST Boulder campus.
- ISC training for all OSY assessors and the individuals responsible for deciding to implement countermeasures and accepting risk. (Recommendation 3)

The NIST Director should finalize and implement risk management policies and procedures, ensuring that they contain a formal coordination mechanism between OSY and NIST and are aligned with Commerce's

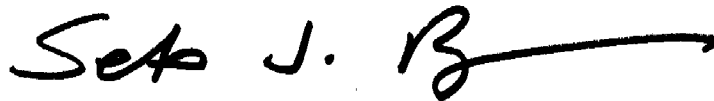
revised risk management policy, particularly with regard to establishing FSCs. (Recommendation 4)

Agency Comments

We provided a draft of the sensitive version of this report to Commerce and DHS for review and comment. In written comments on the sensitive version of this report, Commerce concurred with our four recommendations. Commerce deemed some of the information in the attachment to its original letter to be sensitive. This information was associated with the efforts Commerce has taken to address the security vulnerabilities we identified in our report. Commerce provided a publicly releasable attachment, which we reproduce along with the letter in appendix II. In an e-mail, the DHS audit liaison indicated that DHS would not be providing written comments on the draft report. Commerce and DHS both provided technical comments, which we incorporated as appropriate.

We are sending copies of this report to the appropriate congressional committees, the Secretaries of Commerce and Homeland Security, and other interested parties. In addition, the report is available at no charge on the GAO website at <http://www.gao.gov>.

If you or your staff have any questions about this report, please contact me at (202) 512- 6722 or bagdoyans@gao.gov. GAO staff who made key contributions to this report are listed in appendix III.



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

Appendix I: Methods of Survey of National Institute of Standards and Technology Personnel

To determine the perspectives of scientific and technical employees on the National Institute of Standards and Technology's (NIST) physical security program, we conducted a web questionnaire survey with a statistically representative random sample of 506 nonsecurity NIST employees working in one of six Laboratory Programs at the division level or below at the Gaithersburg and Boulder campuses.

Survey Development

To maximize the utility of estimates for answering our objective, while minimizing respondent burden and total survey error, we developed the survey using a variety of quality-assurance techniques. Survey error can arise from the sampling, population coverage, measurement, nonresponse, and processing errors associated with questionnaire surveys. A GAO statistician and survey specialists determined survey design parameters and developed, tested, revised, and finalized the questionnaire, in consultation with subject-matter experts on the engagement team. The survey design parameters included sample, mode of administration, respondent communication methods, and protection from disclosure of identifiable information.

To minimize measurement error, we pretested the questionnaire using cognitive interviewing techniques, such as nondirective probing of answers and asking respondents to think aloud when formulating answers. This process allowed us to determine whether questions were understood and answered as intended. We conducted in-person pretests with four members of the population at the Boulder campus and seven at the Gaithersburg campus, representing a variety of employee types that would be included in the survey sample. An additional survey specialist, who had not been involved in the development of the questionnaire, also reviewed it. We then modified the questionnaire based on pretest results and suggestions made by the reviewer and subject-matter experts.

The final questionnaire included questions on security training, awareness and knowledge, behaviors observed, institutional commitment to policy, and attitudes on the levels, costs, and benefits of physical security at NIST. Throughout the questionnaire, we defined important terms. For example, we defined the term "physical security," which for the purposes of our work referred to the agency's ability to properly secure its physical facilities and assets. Physical security does not include cybersecurity or laboratory safety measures, other than those that serve to prevent unauthorized access. The survey also presented various scenarios and threats. Additional detail regarding these scenarios and threats was sensitive and is omitted from this report.

Sample Design

The target population—the NIST employees that our survey design represented—included 84 percent of NIST’s nonmanagement, scientific and technical employees. These employees were assigned to one of six Laboratory Programs at the division level or below, and their duty station was either the Boulder or Gaithersburg campus, at the time of our survey.¹ Personnel in our target population included both federal employees of NIST and associates, who include guest researchers, students, and contractors, among other employee types. The target population totaled 3,367 personnel out of a complete list of 7,186 federal employees and associates, provided to us on December 8, 2016, by NIST. The list had characteristics of NIST personnel sufficient to assure us that we had identified all of the personnel in our target population.

From this listing of the target population, we drew a stratified random sample of sufficient size, across six strata, to account for reductions due to nonresponse, ineligibility, and the variability introduced by sampling. The sample of 506 was designed to yield percentage estimates from survey questions generalizable to the overall population with confidence intervals (a measure of sampling error) no wider than ± 7 percentage points at the 95 percent level of confidence, and to the populations represented by each stratum with confidence intervals no wider than ± 10 percentage points, minimizing the sampling error.

The six strata were subgroups of the sample that were combinations of three characteristics of federal or associate personnel type, Boulder or Gaithersburg location, and whether or not the employee or associate worked in highly sensitive facilities. These strata were created so that generalizable estimates with known confidence intervals could be made

¹NIST operates seven primary laboratory programs. There were 626 scientific and technical personnel from one laboratory—NIST’s Information Technology Laboratory—and two staff offices inadvertently excluded from our target population. Subsequent analysis showed that their exclusion did not affect our conclusions. In addition to the seven primary laboratory programs, NIST operates extramural programs under the Associate Director for Innovation and Industry Services, including the Baldrige Performance Excellence Program and the Hollings Manufacturing Extension Partnership. NIST also jointly operates research organizations in four other locations explicitly established to promote cross-disciplinary collaboration. These include JILA, a physics research institute formerly known as the Joint Institute for Laboratory Astrophysics; the Institute for Bioscience and Biotechnology Research; the Joint Quantum Institute; and the Hollings Marine Laboratory. Physical security for these locations is not provided by NIST, and therefore they have been excluded from our scope.

for different groups in the target population, who may have unique perspectives on physical security issues.

Survey Administration and Sample Outcomes

We conducted the web survey from March 17, 2017, through May 9, 2017. To encourage survey participation, we sent sampled personnel a prenotification e-mail describing the survey before sending each of them an e-mail with a unique username and password to their self-administered web questionnaire. NIST also sent an e-mail to all of its personnel notifying them of the GAO survey before it began, and encouraging them to participate if they were randomly selected into the survey.

The file NIST provided, from which we drew our sample, contained e-mail addresses and phone numbers for all federal employees. However, no e-mail addresses were on file for 147 associates among the 506 personnel we sampled, so we first sent notification e-mails to the 359 sampled personnel for whom e-mail addresses were available. We sent a second wave of notification e-mails on March 29, 2017, to the remaining 134 personnel for whom NIST subsequently found e-mail addresses.² These individuals were typically associates who no longer held a NIST e-mail address. To identify their personal e-mail address, NIST asked their supervisors or sponsors for contact information. For those whose e-mails were returned to us as undeliverable, we asked NIST to provide correct e-mail addresses and confirm their current eligibility as personnel in our target population. During survey administration, we attempted to call sampled personnel that had not yet completed the survey (nonrespondents) to determine their eligibility, update their contact information, answer any questions or concerns they had about taking the survey, and obtain their commitment to participate. We also sent multiple follow-up e-mails to nonrespondents encouraging response, and providing instructions for taking the web-based survey, further minimizing the possibility of nonresponse error.

On the basis of NIST's search for contact information for those with undeliverable e-mail addresses, and nonresponse follow-up we conducted during the survey, we determined that 29 sampled people were no longer eligible as members of the target population. Sample members were deemed ineligible if we confirmed that they were no longer

²NIST was unable to identify e-mail addresses for 13 personnel included in our sample.

employed by or affiliated with NIST and not in possession of a NIST access card at the time the survey began, or when we were first able to contact them.

At the end of survey administration, we had obtained 274 usable questionnaires, which in addition to completed questionnaires included 11 partial responses that were considered usable for our analysis because a sufficient number of questions had been answered. The unweighted response rate, calculated as the number of usable responses divided by the remaining 477 from the original sample that were known to be or assumed to be eligible, was 57 percent. However, because it is likely that there were also ineligible among the nonrespondents, we can also assume that a proportion of nonrespondents of unknown eligibility were also ineligible; we assume that this proportion is the same as among those of known eligibility and ineligibility. When we removed these additional nonrespondents assumed to be ineligible from our calculations and statistically adjusted, or weighted, this eligibility-adjusted response rate within each stratum, the overall response rate was 62 percent.³ Table 2 illustrates the sample size, eligibility determination, and unweighted and weighted response rates across each stratum and overall.

Table 2: Survey Population, Sample, and Outcomes

| Stratum | Target population | Original sample | Ineligible | Eligible sample | Usable responses | Adjusted response rate ^a (percent) |
|---|-------------------|-----------------|------------|-----------------|------------------|---|
| Associates in Boulder | 361 | 94 | 10 | 84 | 54 | 68 |
| Federal employees in Boulder | 283 | 78 | 2 | 76 | 42 | 56 |
| Associates in Gaithersburg | 921 | 56 | 12 | 44 | 31 | 77 |
| Federal employees in Gaithersburg | 982 | 102 | 2 | 100 | 61 | 62 |
| Associates in the highly sensitive group | 645 | 135 | 2 | 133 | 61 | 47 |
| Federal employees in the highly sensitive group | 175 | 41 | 1 | 40 | 25 | 63 |
| Total | 3,367 | 506 | 29 | 477 | 274 | 62^b |

Source: GAO. | GAO-18-95

Note: Data are from GAO survey of NIST employees.

^aResponse rate is adjusted to include an estimated proportion of cases of unknown eligibility that are actually ineligible (American Association of Public Opinion Research Response Rate 3, defined at <http://www.aapor.org/Publications-Media/AAPOR-Journals/Standard-Definitions.aspx>).

³See discussion of statistical weighting in the “Survey Results” section below.

^bThe overall response rate is weighted to take into account unequal sampling rates between strata. Dividing the number of respondents by the total survey population will not result in the response rate, due to weighting.

In addition to nonresponse error leading to imprecision of estimates because fewer observations are made, nonresponse bias in survey estimates can arise if many of those who do not respond would have given responses different from those who did. We compared response rates across categories of location, personnel type, and program, which are characteristics likely to be associated with answers to some questions, and found no statistically significant difference in those response rates. None of those characteristics affect the likelihood to respond; so we conclude there is no evidence of nonresponse bias.

We statistically adjusted, or weighted, survey results to multiply the contribution of each responding member of the sample, to produce estimates that represent the entire target population of NIST personnel as defined above. Different weights must be applied to the respondents within each stratum, because the numbers sampled from, and responding in a stratum, may be relatively small or large compared to the total population in that stratum. Therefore, some respondent answers must be multiplied by larger or smaller weighting factors depending on the stratum.

Because we followed a probability procedure based on random selections, our sample is only one of a large number of samples that we might have drawn. As each sample could have provided different estimates, we express our confidence in the precision of our particular samples' results as 95 percent confidence intervals (e.g., from a lower bound to an upper bound). This is the interval that would contain the actual population value for 95 percent of the samples we could have drawn. As a result, we are 95 percent confident that each of the confidence intervals based on our survey includes the true values in the sample population.

Finally, to minimize the possibility of processing error, all data-processing and analysis programming was verified by a separate statistician. On the basis of our application of quality-assurance and control practices, we determined that the survey data were of sufficient reliability for our purposes.

Survey Results

Our survey was composed of questions with predetermined answer choices (closed-ended questions) and questions without predetermined answer choices requiring a written response (open-ended questions). The details and responses (including the text of all survey questions, aggregate, results, and associated confidence intervals for closed-ended questions) are sensitive and have been omitted from this report.

Appendix II: Comments from the Department of Commerce



UNITED STATES DEPARTMENT OF COMMERCE
The Secretary of Commerce
Washington, D.C. 20230

September 14, 2017

Mr. Seto J. Bagdoyan
Director, Audits
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Bagdoyan:

Thank you for the opportunity to review and comment on the Government Accountability Office's (GAO) draft report titled *Physical Security: NIST and Commerce Need to Complete Efforts to Address Persistent Challenges* (GAO-18-14SU), dated October 2017. We appreciate your team's assessment of the National Institute of Standards and Technology's physical security programs as the Department of Commerce is committed to the security and safety of our personnel, facilities, information, and assets.

The Department agrees with the full extent of the report's recommendations. Enclosed you will find both formal comments as well as technical comments and recommendations for consideration to amend the draft report as appropriate.

If you have any questions, please contact Richard Townsend, Acting Director for Security, at (202) 482-7897 or RTownsend@doc.gov.

Sincerely,

A handwritten signature in blue ink that reads "Wilbur Ross".

Wilbur Ross

Enclosures
Department of Commerce Formal Comments
Department of Commerce Technical Comments

**Department of Commerce's Comments on
the Government Accountability Office (GAO) Draft Report entitled *Physical Security:
NIST and Commerce Need to Complete Efforts to Address Persistent Challenges*
(GAO-18-95)**

The Department of Commerce (Department) has reviewed the draft report, and we offer the following comments for GAO's consideration.

Comments on Recommendations

The Department concurs with the four recommendations in the draft GAO report, NIST Physical Security (GAO-18-95), dated October 2017.

- **Recommendation 1:** The NIST Director should incorporate elements of key practices into the implementation of the Security Sprint action plans, by establishing a comprehensive communication strategy for employees; interim milestone dates; and measures to assess effectiveness.
- **Recommendation 2:** The Director of the OSY, in coordination with the NIST Director, should conduct an evaluation of the effectiveness of the current security management structure as compared to a consolidated security structure, centrally managed by OSY, to identify the most effective and feasible approach to physical security at NIST.
- **Recommendation 3:** The Director of OSY should ensure that the draft Commerce risk management policy is finalized and implemented in accordance with the ISC's Risk Management Process Standard.
- **Recommendation 4:** The NIST Director should finalize and implement risk management policies and procedures, ensuring that they contain a formal coordination mechanism between OSY and NIST and are aligned with Commerce's revised risk management policy, particularly with regard to establishing Facility Security Committees (FSC).

General Comments

Prior to and during the GAO's review, the Department has acted proactively to implement solutions to mitigate vulnerabilities identified by GAO in the draft report. The Department is committed to establishing an action plan to address the recommendations of the Final Report, to enhance physical security at NIST, and improve the effectiveness of the Department's physical security program. For example, the Department and NIST have already begun efforts to increase awareness of security programs with scheduled Security Awareness Days in 2017.

The Department is also revising its Risk Management Process (RMP) policy and the new policy will detail its alignment with the Interagency Security Committee (ISC) RMP Standard and other

Commerce-specific best practices, such as mandatory ISC RMP training for all assessors performing Facility Security Assessments (FSAs).

Additionally, the Department will implement a new FSA process and report template in FY18. Like the new RMP, this new process and report template is designed to align Commerce's physical security risk assessment processes with the ISC RMP Standard. Moreover, the Department is managing and will maintain an appropriate level of qualified security assessment staff who will be certified through the ISC RMP Standard course. To date, the Department has increased its ISC RMP-trained staff from 4 to 16, and by September 30, 2017, OSY plans to have 21 trained risk assessment personnel.

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contact

Seto J. Bagdoyan, (202) 512-6722 or bagdoyans@gao.gov

Staff Acknowledgments

In addition to the contact named above, Gabrielle Fagan (Assistant Director); Elizabeth Kowalewski (Analyst in Charge); Elizabeth Dretsch, Justin Fisher, April Gamble, Amber D. Gray, Georgette Hagans, James Murphy, Carl Ramirez, and Shana Wallace made key contributions to this report. Other contributors include Maurice Belding, Laurie Chin, Colin Fallon, Robert Graves, Barbara Lewis, Jason Lyuke, Maria McMullen, Nada Raof, Ramon Rodriguez, Julie Spetz, and Helina Wong.

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



Please Print on Recycled Paper.