



Report to the Committee on Oversight
and Government Reform, House of
Representatives

October 2017

FEDERAL FACILITY SECURITY

Selected Agencies Should Improve Methods for Assessing and Monitoring Risk

Accessible Version

GAO Highlights

Highlights of [GAO-18-72](#), a report to the Committee on Oversight and Government Reform, House of Representatives

Why GAO Did This Study

Protecting federal employees and facilities from security threats is of critical importance. Most federal agencies are generally responsible for their facilities and have physical security programs to do so.

GAO was asked to examine how federal agencies assess facilities' security risks. This report examines: (1) how selected agencies' assessment methodologies align with the ISC's risk management standard for identifying necessary countermeasures and (2) what management challenges, if any, selected agencies reported facing in conducting physical security assessments and monitoring the results.

GAO selected four agencies—CBP, FAA, ARS, and the Forest Service—based on their large number of facilities and compared each agency's assessment methodology to the ISC Standard; analyzed facility assessment schedules and results from 2010 through 2016; and interviewed security officials. GAO also visited 13 facilities from these four agencies, selected based on geographical dispersion and their high risk level.

What GAO Recommends

GAO recommends: (1) that CBP and FAA update policies to require the use of methodologies fully aligned with the ISC Standard; (2) that CBP revise its plan to eliminate the assessments backlog; and (3) that all four agencies improve monitoring of their physical security programs. All four agencies agreed with the respective recommendations.

View [GAO-18-72](#). For more information, contact Lori Rectanus at (202) 512-2834 or rectanusl@gao.gov.

October 2017

FEDERAL FACILITY SECURITY

Selected Agencies Should Improve Methods for Assessing and Monitoring Risk

What GAO Found

None of the four agencies GAO reviewed—U.S. Customs and Border Protection (CBP), the Federal Aviation Administration (FAA), the Agricultural Research Service (ARS), and the Forest Service—used security assessment methodologies that fully aligned with the Interagency Security Committee's *Risk Management Process for Federal Facilities* standard (the ISC Standard). This standard requires that methodologies used to identify necessary facility countermeasures—such as fences and closed-circuit televisions—must:

1. Consider all of the undesirable events (i.e., arson and vandalism) identified by the ISC Standard as possible risks to facilities.
2. Assess three factors—threats, vulnerabilities, and consequences—for each of these events and use these three factors to measure risk.

All four agencies used methodologies that included some ISC requirements when conducting assessments. CBP and FAA assessed vulnerabilities but not threats and consequences. ARS and the Forest Service assessed threats, vulnerabilities, and consequences, but did not use these factors to measure risk. In addition, the agencies considered many, but not all 33 undesirable events related to physical security as possible risks to their facilities. Agencies are taking steps to improve their methodologies. For example, ARS and the Forest Service now use a methodology that measures risk and plan to incorporate the methodology into policy. Although CBP and FAA have updated their methodologies, their policies do not require methodologies that fully align with the ISC standard. As a result, these agencies miss the opportunity for a more informed assessment of the risk to their facilities.

All four agencies reported facing management challenges in conducting physical security assessments or monitoring assessment results. Specifically, CBP, ARS, and the Forest Service have not met the ISC's required time frame of every 3 years for conducting assessments. For example, security specialists have not conducted required reassessments of two ARS and one Forest Service higher-level facilities. While these three agencies have plans to address backlogs, CBP's plan does not balance conducting risk assessments with other competing security priorities, such as updating its policy manual, and ARS and the Forest Service lack a means to monitor completion of future assessments. Furthermore, CBP, ARS, and the Forest Service did not have the data or information systems to monitor assessment schedules or the status of countermeasures at facilities, and their policies did not specify such data requirements. For example, ARS and the Forest Service do not collect and analyze security-related data, such as countermeasures' implementation. FAA does not routinely monitor the performance of its physical security program. Without improved monitoring, agencies are not well equipped to prioritize their highest security needs, may leave facilities' vulnerabilities unaddressed, and may not take corrective actions to meet physical security program objectives. This is a public version of a sensitive report that GAO issued in August 2017. Information that the agencies under review deemed sensitive has been omitted.

Contents

Letter	1
Background	4
Selected Agencies' Assessment Methodologies Do Not Fully Align with the ISC's Risk Management Standard	8
Selected Agencies Reported Facing Challenges in Conducting Security Assessments and Monitoring Results	15
Conclusions	23
Recommendations for Executive Action	24
Agency Comments	25
Appendix I: Objectives, Scope, and Methodology	27
Appendix II: Selected Facilities GAO Visited	32
Appendix III: The Interagency Security Committee's Undesirable Events	33
Appendix IV: Comments from the Department of Homeland Security	35
Appendix V: Comments from the Department of Transportation	39
Appendix VI: Comments from the Department of Agriculture	40
Appendix VII: GAO Contact and Staff Acknowledgments	41
Appendix VIII: Accessible Data	42
Agency Comment Letters	42

Tables

Table 1: Comparison of Selected Agencies' Policies and Assessment Methodologies with the Interagency Security Committee's (ISC) Standard, Risk Management Process for Federal Facilities	9
Table 2: Selected Agencies Prioritize Operational Needs over Physical Security Needs	14
Table 3: Limitations of Agencies' Information and the Effect on Facility Security	18

Table 4: 13 Facilities GAO Visited at the Department of Homeland Security (DHS), U.S. Customs and Border Protection (CBP); Department of Transportation (DOT), Federal Aviation Administration (FAA); and the United States Department of Agriculture (USDA), Agricultural Research Service (ARS) and the Forest Service	32
Table 5: The Interagency Security Committee's Undesirable Events	33

Figures

Figure 1: Elements of Risk Management	4
Figure 2: The Interagency Security Committee's (ISC) Risk Management Process	6
Figure 3: Examples of Recommended Physical Security Countermeasures Not Fully Implemented at Selected Facilities	22

Abbreviations

ARS	Agricultural Research Service
CBP	U.S. Customs and Border Protection
DHS	Department of Homeland Security
DOT	Department of Transportation
FAA	Federal Aviation Administration
ISC	Interagency Security Committee
USDA	U.S. Department of Agriculture

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 26, 2017

The Honorable Trey Gowdy
Chairman
The Honorable Elijah E. Cummings
Ranking Member
Committee on Oversight and Government Reform
House of Representatives

Several incidents—such as armed citizens taking over a federal wildlife refuge in Oregon for about 40 days in 2016; the active shooter incident at the Washington Navy Yard in Washington, D.C., in 2013 that resulted in several deaths; and the fatal shooting at the Anderson Federal Building in Long Beach, California, in 2012—demonstrate that government facilities and their employees continue to be targets of potential harm.¹ In light of these incidents and other emergent threats, it is important that agencies use risk-based methodologies to assess the physical security needs of the approximately 113,000 executive-branch, non-military federal buildings.² Security assessments of facilities can uncover vulnerabilities and threats and recommend protective measures—called countermeasures—such as fences, access control systems, and closed-circuit television systems to mitigate those threats.

At least 30 federal agencies are responsible for protecting about 45 percent of civilian federal facilities and their occupants from potential threats. To help federal agencies protect and assess risks to their facilities, the Interagency Security Committee (ISC), an organization chaired by the Department of Homeland Security (DHS), developed

¹This report refers to buildings and facilities in the United States occupied by federal employees for nonmilitary activities as “federal facilities.”

²Federal Real Property Council, *FY 2015 Federal Real Property Report* (the most recent report available.) The figure provided excludes military assets. In recent work, we assessed the reliability of *Federal Real Property Report*’s data and found problems with data collection practices. See GAO, *Federal Real Property: Improving Data Transparency and Expanding the National Strategy Could Help Address Long-standing Challenges*, [GAO-16-275](#) (Washington: D. C.: Mar. 31, 2016) and GAO, *Facility Security: Greater Outreach by DHS on Standards and Management Practices Could Benefit Federal Agencies*, [GAO-13-222](#) (Washington: D. C.: Jan. 24, 2013). However, we found the data to be reliable for the purposes of providing a broad overview of the makeup of the government’s federal real property portfolio.

physical security standards for non-military federal facilities in the United States.

One particular standard, called *The Risk Management Process for Federal Facilities*, defines the criteria and process executive agencies and departments must follow when assessing risks to their facilities.³ However, our past work found that some federal agencies used this standard to varying degrees leaving agencies' facilities, workforce, and visitors exposed to risk.⁴ You asked us to examine how federal agencies with protective responsibilities use risk management to protect their facilities with countermeasures that meet their security needs. This report examines (1) how selected agencies' assessment methodologies align with the ISC risk management standard to identify necessary countermeasures, and (2) what management challenges, if any, selected agencies reported facing in conducting physical security assessments and monitoring the results.

This product is a public version of a sensitive report that we issued in August 2017.⁵ DHS deemed some of the information in our August report to be sensitive, including information about facility locations, risk assessment results, and undesirable events not assessed for federal facilities physical security. Therefore, this report omits that information which must be protected from public disclosure. 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 address the objectives, we selected four agencies with responsibility for assessing their own facilities—DHS's U.S. Customs and Border Protection (CBP); the Department of Transportation's Federal Aviation Administration (FAA); and the United States Department of Agriculture's

³ISC, *The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard* (Washington, D. C.: November 2016). The ISC Standard incorporates the following appendixes; Appendix A: The Design-Basis Threat Report; Appendix B: Countermeasures; Appendix C: Child-Care Centers Level of Protection Template.

⁴GAO, *Federal Facility Security: Additional Actions Needed to Help Agencies Comply with Risk Assessment Methodology Standards*, [GAO-14-86](#) (Washington, D. C.: Mar. 5, 2014).

⁵ GAO, *Facility Security: Agencies Should Improve Methods for Assessing and Monitoring Risk* [GAO-17-605SU](#), Washington, D.C.: Aug. 9, 2017)

(USDA) Agricultural Research Service (ARS) and Forest Service.⁶ To determine how these agencies' assessment methodologies align with *The Risk Management Process for Federal Facilities* (the ISC Standard), we compared facility security policies and procedures from the departments and agencies to the criteria and process in the ISC Standard. In addition, we selected 13 facilities within these 4 agencies for site visits based on geographical dispersion and high levels of risk. For each of the selected facilities, we reviewed assessment reports, toured the facilities, and identified the status of recommended countermeasures. We interviewed officials from the ISC, 3 departments, 4 agencies, and the 13 facilities to understand security standards, policies, and procedures; agency-specific assessment processes; management challenges; and guidance for prioritizing physical security needs. We did not independently determine what constitutes a management challenge, but relied on these facility managers and agency security staff to identify their concerns as defined in their own policies and procedures. We reviewed *Standards for Internal Control in the Federal Government (Standards for Internal Control)* regarding risk management criteria and the use of quality information for our evaluation of the agencies' abilities to monitor their physical security program.⁷ The results of our review of the selected agencies are not generalizable to all the ISC member agencies but provide illustrative examples of risk assessments and how the facilities addressed needed countermeasures. See appendix I for more details on our scope and methodology and appendix II for a list of the 13 selected facilities visited.

The performance audit upon which this report is based was conducted from June 2016 to August 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 subsequently worked with DHS, DOT, and USDA from August 2017 to October 2017 to prepare this version of the sensitive report for public release. This public version was also prepared in accordance with these standards.

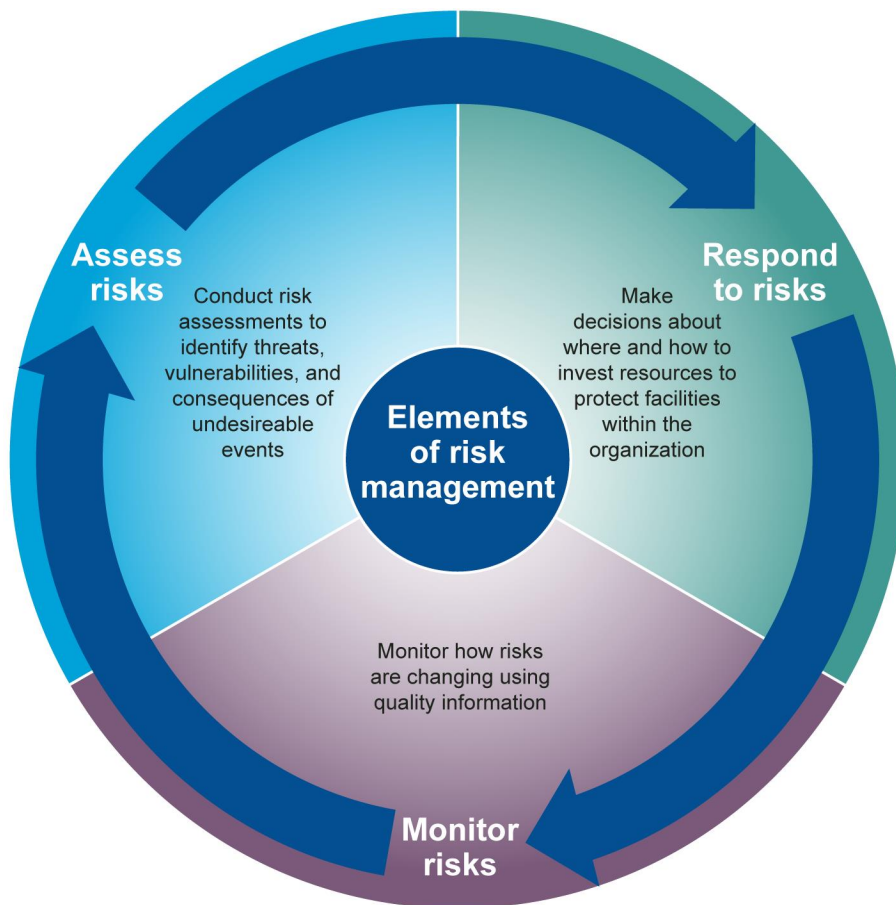
⁶We selected agencies based on the large number of controlled facilities and facilities within these agencies based on security levels, geographical dispersion and type of facilities.

⁷GAO, *Standards for Internal Control in the Federal Government*, [GAO-14-704G](#) (Washington, D. C.: September 2014).

Background

Risk management, as applied to security of federal facilities, entails a continuous process of applying a series of mitigating actions—assessing risk through the evaluation of threats, vulnerabilities, and consequences; responding to risks with appropriate countermeasures; and monitoring risks using quality information (see fig. 1).⁸

Figure 1: Elements of Risk Management



Source: GAO. | GAO-18-72

⁸GAO, *Enterprise Risk Management: Selected Agencies' Experiences Illustrate Good Practices in Managing Risk*, [GAO-17-63](#) (Washington, D.C.; Dec. 1, 2016).

In 1995, Executive Order 12977 established the ISC after the bombing of the Oklahoma City Alfred P. Murrah Federal Building in April 1995.⁹ The ISC's mandate is to enhance the quality and effectiveness of security in and protection of federal facilities in the United States occupied by federal employees for nonmilitary activities.¹⁰ The order directs the ISC to develop and evaluate security standards for federal facilities, develop a strategy to ensure executive agencies and departments comply with such standards,¹¹ and oversee the implementation of appropriate security measures in federal facilities. The ISC has released a body of standards, including the ISC Standard, designed to apply to the physical security efforts of all federal, non-military agencies.¹² The ISC Standard prescribes a process for agencies to follow in developing their risk assessment methodologies (see fig. 2).

Most federal departments and agencies are generally responsible for protecting their own facilities and have physical security programs in place to do so.¹³ The ISC Standard requires executive departments and agencies to follow the risk-management process when conducting risk assessments for each of their facilities. That process begins with determining the facility security level, ranging from level I (lowest risk) for facilities generally having 100 or fewer employees to level V (highest risk) for the most critical facilities and generally having greater than 750 employees. The security level designation determines the facility's

⁹Executive Order 12977, 60 Fed. Reg. 54411 (Oct. 24, 1995), as amended by Executive Order 13286, 68 Fed. Reg. 10619 (Mar. 5, 2003) which, among other things, transferred the responsibility for chairing the committee from the Administrator of the General Services Administration to the Secretary of Homeland Security. ISC members consist of about 60 federal departments and agencies, as of March 2017.

¹⁰Executive Order 12977 refers to buildings and facilities in the United States occupied by federal employees for non-military activities as "federal facilities." In this report, we acknowledge that a single facility may involve several buildings.

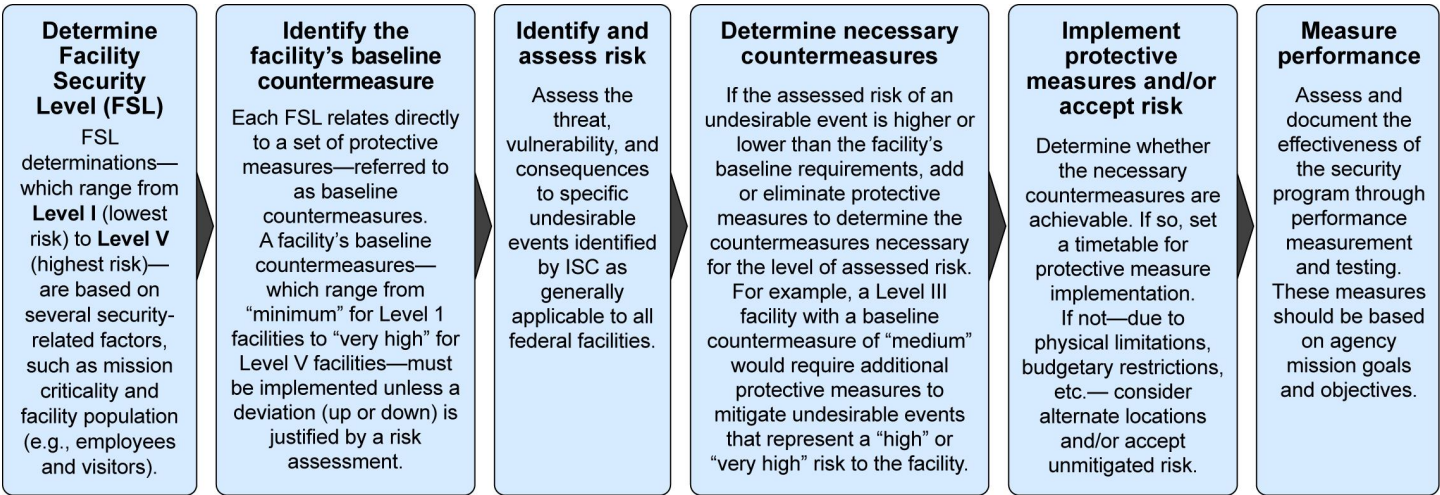
¹¹Pursuant to Executive Order 12977, as amended, executive agencies and departments are exempt from complying with ISC policies and recommendations "where the Director of Central Intelligence determines that compliance would jeopardize intelligence sources and methods."

¹²Physical security standards for military facilities are covered by the Department of Defense's *Unified Facility Criteria* and overseas nonmilitary facilities are covered by the State Department's *Foreign Affairs Manual for Physical Security of Facilities Abroad* (12 FAM 310).

¹³The Federal Protective Service protects about 9,000 federal facilities, including buildings and structures; this figure is a small portion of the over 100,000 executive branch, non-military, federal buildings.

baseline countermeasures.¹⁴ For each facility, departments and agencies are required to (a) consider all of the “undesirable events” that could pose a risk to their facilities— such as active shooters, vandalism, and explosions—and (b) assess three factors of risk (threats, vulnerabilities, and consequences) to specific undesirable events.¹⁵ Subsequently, agencies are to combine all three factors to yield a measurable level of risk for each undesirable event (see app. III). Based on the results of these assessments, agencies should customize (either increase or decrease) the countermeasures to adequately reflect the assessed level of risk.

Figure 2: The Interagency Security Committee’s (ISC) Risk Management Process



Source: GAO analysis of Interagency Security Committee information. | GAO-18-72

In addition, as part of planning for physical security resources within an agency's budget process, the ISC has identified the need to balance allocations for countermeasures with other operational needs and with

¹⁴ISC, *The Risk Management Process for Federal Facilities: An Interagency Security Committee: Appendix B: Countermeasures* (May 2017).

¹⁵Threats are the intentions and capabilities of adversaries to initiate undesirable events; consequences are the level, duration, and nature of losses resulting from undesirable events; vulnerabilities are weaknesses in the design or operation of a facility that adversaries can exploit. Undesirable events represent the “reasonable worst case scenario” for each threat. Risk assessment methodologies involve assigning ratings to each of the three factors and combining these ratings to produce an overall measurement of risk for each identified undesirable event.

competing priorities.¹⁶ The ISC Best Practices have some similarities with leading practices in capital decision-making. For example, both state that the allocation of resources should be integrated into the agency's mission, objectives, goals, and budget process. However, beyond the ISC Best Practices, the Office of Management and Budget and we have developed more comprehensive leading practices in capital decision-making that provide agencies with guidance for prioritizing budget decisions such as for countermeasure projects.¹⁷ The Office of Management and Budget and our guidance also emphasize evaluating a full range of alternatives, informed by agency asset inventories that contain condition information, to bridge any identified performance gap. Furthermore, the guidance calls for a comprehensive decision-making framework to review, rank, and select from among competing project proposals. Such a framework should include the appropriate levels of management review, and selections should be based on the use of established criteria.

The following describes the mission and physical security program characteristics for the agencies in our review:¹⁸

- CBP, the nation's largest law enforcement agency, has responsibility for securing the country's borders. It also has responsibility for conducting security assessments at about 1,200 facilities, including approximately 215 federally owned and agency-controlled higher-level facilities (facility security levels III and IV). These facilities include border patrol stations with holding cells for people detained at the border, office buildings, and canine-training centers. CBP conducts these assessments.
- FAA's mission is to provide a safe and efficient aerospace system for the country. According to agency data, FAA has 55 federally owned and agency-controlled higher-level facilities—including critical air

¹⁶ISC, *Best Practices for Planning and Managing Physical Security Resources: An Interagency Security Committee Guide* (Washington, D. C.: December 2015).

¹⁷According to leading practices established by OMB and GAO: Office of Management and Budget, *Supplement to Circular No. A-11, Part 7, Capital Programming Guide* (Washington, D.C.: July 2016) and GAO, *Executive Guide: Leading Practices in Capital Decision-Making*, [GAO/AIMD-99-32](#) (Washington, D.C.: December 1998).

¹⁸As executive branch agencies, CBP, FAA, ARS, and the Forest Service are to follow the ISC standards.

traffic control towers. According to FAA officials, FAA specialists conduct security assessments.

- ARS conducts research related to agriculture and disseminates information to ensure high-quality safe food and to sustain a competitive agricultural economy. According to agency data, ARS has security responsibility for four domestic federally owned and agency-controlled higher-level facilities—including laboratories for research to improve food and crop quality, office buildings, and warehouses. ARS security personnel have responsibility for conducting security assessments.¹⁹
- The Forest Service sustains the health, diversity, and productivity of the nation's forests and grasslands. According to agency officials, the Forest Service has one federally owned and agency-controlled higher-level facility—a regional headquarters office building. The Forest Service's security officials have responsibility for conducting security assessments, but at the time of our review, USDA security officials conducted the assessment at Forest Service's one higher-level facility.²⁰

Selected Agencies' Assessment Methodologies Do Not Fully Align with the ISC's Risk Management Standard

None of the four selected agencies' security assessment methodologies fully aligned with the ISC Standard. The ISC gives agencies some flexibility to design their own security-assessment methodologies for identifying necessary countermeasures as long as the chosen methodology adheres to fundamental principles of a sound risk-management methodology. Specifically, methodologies must:

- consider all of the undesirable events identified in the ISC Standard as possible risks to federal facilities, and

¹⁹At the time of our review, USDA security officials conducted most of ARS's assessments.

²⁰The Forest Service's security officials conduct assessments at the agency's lower-level facilities using USDA guidance.

- assess three factors of risk (threats, vulnerabilities, and consequences) for each of the events.²¹

Furthermore, the ISC Standard requires executive departments and agencies to document decisions that deviate from the ISC Standard. Agencies' policies and methodologies reference the ISC Standard. However, none of the agencies' methodologies considered all of the undesirable events during assessments although they used some type of risk assessment methodology.²² In addition, the agencies did not always adhere to these principles of risk management (see table 1).

Table 1: Comparison of Selected Agencies' Policies and Assessment Methodologies with the Interagency Security Committee's (ISC) Standard, Risk Management Process for Federal Facilities

Selected agency	Do policies and methodologies reference the ISC Standard?	Does the methodology consider all 33 undesirable events?	Does the methodology assess the threat of any undesirable events?	Does the methodology assess the vulnerability of any undesirable events?	Does the methodology assess the consequence of any undesirable events?
U.S. Customs and Border Protection (CBP) ^a	Y	N	N	Y	N
Federal Aviation Administration (FAA) ^b	Y	N	N	Y	N
Agricultural Research Service (ARS) ^c	Y	N	Y	Y	Y
Forest Service	Y	N	Y	Y	Y

Source: GAO analysis of agency information. | GAO 18-72

^aCBP and other Homeland Security components are to follow the department's physical security policy, which incorporates the ISC Standard. See Department of Homeland Security, Instruction Manual 121-01-010-01, Rev 1, July 21, 2014.

^bThe Department of Transportation's physical security policy references the ISC Standard, but the policy does not apply to FAA. See Department of Transportation, Facilities Protection Program, Order 1600.26B, January 31, 2013.

^cARS and the Forest Service follow departmental security policies for conducting security assessments.

²¹ISC, *The Risk Management Process for Federal Facilities* (August 2013) listed 31 undesirable events. Its November 2016 revision adds 3 and deletes 1 for a total of 33 undesirable events. We limited the scope of this analysis to these two elements because agencies' adherence to these standards could be objectively verified by reviewing and analyzing agency documentation and interviewing agency officials. See appendix I for more details on our scope and methodology.

²²We omitted specific details because the information is considered sensitive.

At the time of our review, CBP's methodology did not fully align with the ISC Standard because it did not consider all of the 33 undesirable events nor assess threat and consequence. CBP security specialists assessed vulnerabilities at building entrances and exits, in interior rooms, and around the perimeter using a yes/no checklist during the assessment process. However, assessment reports showed that specialists did not assess the threats and consequences of undesirable events at each facility. According to security officials, the gap occurred because they designed the checklist to meet requirements in the 2009 *CBP Security Policy and Procedures Handbook*,²³ which predates the first edition of the ISC Standard issued in 2010. CBP officials told us that as of January 2017, they began using an improved methodology to assess the threats, vulnerabilities, and consequences for 30 of 33 undesirable events—omitting three now identified in the November 2016 revision to the ISC Standard. However, CBP has not yet updated its handbook to align with the ISC Standard, even though it started this effort over 3 years ago in December 2013. CBP officials did not provide a draft of its updated handbook, but they provided a plan with milestone dates for issuing the handbook by September 2018. CBP officials also told us that updates to the handbook may have to wait due to competing priorities, including efforts to address the backlog of assessments (which we discuss later in this report). Delays in updating the handbook mean that CBP's policy will continue to not align with the ISC Standard. Furthermore, although CBP security officials told us that all of the agency's security specialists have been trained to use the improved assessment methodology, without documentation of the methodology in agency policy, there may be greater risk of its inconsistent application. *Standards for Internal Control* emphasize the importance of agencies developing and documenting policies to ensure agency-wide objectives are met. Documentation serves to retain institutional knowledge over time when questions about previous decisions arise. Without an updated policy handbook that requires a methodology that assesses all undesirable events consistent with the ISC Standard, CBP cannot reasonably ensure that its facilities will have levels of protection commensurate to their risk.

FAA's methodology does not fully align with the ISC Standard because it does not consider all of the 33 undesirable events nor does it assess all

²³U.S. Customs and Border Protection, *CBP Security Policy and Procedures Handbook*, HB1400-02B (Aug. 13, 2009) and Interagency Security Committee, *Physical Security Criteria for Federal Facilities: An Interagency Security Committee Standard* (Apr. 12, 2010).

three factors of risk. FAA security specialists assess vulnerabilities to the site perimeter, entryways, and interior rooms using a yes/no checklist, but the checklist does not assess the consequences from each of the undesirable events at each facility. With respect to threat, FAA applies the ISC's baseline threat—a general federal facilities threat level that relates directly to a set of baseline countermeasures—across all its higher-level facilities because FAA policy states that there is no agency-specific threat that exceeds the current baseline threat.²⁴ According to FAA officials, the baseline threat standardizes the security needs across their facilities rather than addressing the security needs of individual facilities from specific threats. When necessary, FAA policy allows specialists to modify countermeasures based on an evaluation of conditions at the facility.

FAA realized that this approach was no longer appropriate given the agency-wide goal to make risk-based decisions, a review of the assessment process after a 2014 Chicago fire incident that destroyed critical FAA equipment, and an awareness of ISC initiatives to assess compliance. To address the resulting methodological gaps, FAA hired a contractor to design, develop, test, and validate an improved risk-assessment methodology. Subsequently, FAA improved its methodology in January 2017 to assess the threats, vulnerabilities, and consequences for 30 of the 33 undesirable events identified in the November 2016 revision to the ISC Standard²⁵—and tested the methodology at lower- and higher-level facilities. This revised methodology addresses the need to assess individual facility needs rather than using a standardized baseline approach. In April 2017, FAA officials told us of their plan for implementing this methodology and provided tentative milestone dates to conduct further testing, training, and analysis before deciding to use the improved methodology, which they expect to complete by January 2018. However, their plan lacks the necessary information to ensure successful implementation, such as detail on how many facilities they will test and how they will use the results of testing, training, and analysis to implement the improved methodology within the identified 9-month time frame. Furthermore, the improved methodology does not address undesirable events for which ISC issued countermeasures in May 2017.

²⁴Federal Aviation Administration, FAA Facility Security Management Program, Order 1600.69C, August 22, 2016.

²⁵FAA's methodology does not include the three undesirable events now identified in the November 2016 revision to the ISC Standard because officials said that the ISC had not yet identified countermeasures for them. In May 2017, the ISC issued countermeasures for these undesirable events.

Without a detailed implementation plan to assess the methodology's impact on its security program, FAA cannot reasonably ensure that its facilities have the proper countermeasures. With ongoing changes to its security program, FAA has an opportunity to fully align its improved methodology with the ISC Standard by including all 33 undesirable events and to update its policy requiring the use of such a methodology.

Unlike CBP and FAA—which developed their own methodologies separate from their parent departments (Department of Homeland Security (DHS) and Department of Transportation (DOT), respectively)—ARS and the Forest Service follow an assessment methodology developed by USDA. USDA's methodology does not fully align with the ISC Standard because it does not consider all of the 33 undesirable events for which ISC issued countermeasures in May 2017. Security specialists from USDA headquarters typically assess ARS's and the Forest Service's higher-level facilities using a risk-based methodology that considers the 31 undesirable events listed in the previous version of the ISC Standard dated August 2013. However, until recently, USDA did not assign ratings to each of the three risk factors—threat, vulnerability, and consequence—and then combine these ratings to yield a measurable level of risk for each undesirable event. USDA security officials said that they have revised the assessment-reporting format to include this risk calculation and trained their specialists to measure risk in this way. USDA officials provided us with a new assessment template that addresses all 33 undesirable events and includes measuring risk. Additionally, USDA officials said that they are revising their outdated physical security manual and expect to complete it by April 2018. With a revised manual and application of the new assessment template, USDA should be better positioned to assess risk at its facilities.

When agencies do not use methodologies that fully align with the ISC Standard, they could face deleterious effects, ranging from facilities having inappropriate levels of protection to agencies having an inability to make informed resource allocation decisions for their physical security needs. Specifically, the ISC Standard states that facilities may face the effect of either having (1) less protection than needed resulting in inadequate security or (2) more protection than needed resulting in an unnecessary use of resources. The ISC Standard also states that these effects can be negated by determining the proper protection according to a risk assessment. Identified excess resources in one risk area then can be reallocated to underserved areas, thus ensuring the most cost-effective security program is implemented. As an illustration of such potential effects, we found that two agencies assessing two higher-level

facilities came to two different conclusions in terms of their need for X-ray machines to screen for guns, knives, and other prohibitive items in federal facilities. Specifically, one agency based its decision on a policy that does not deviate from the ISC's baseline set of countermeasures, and the other agency based its decision on professional judgement that deviated from the ISC's baseline set of countermeasures. Neither agency based its decision on a risk assessment nor documented its decision—both ISC requirements, specifically:

- Without conducting a risk assessment, FAA recently expanded a policy requirement calling for all higher-level facilities to have X-ray machines and magnetometers. This new requirement poses a potentially sizeable investment for the agency with an estimated cost of X-ray machines of about \$24,000 and magnetometers of about \$4,000 each. FAA may need such equipment at all its higher-level facilities. However, the ISC Standard requires that agencies conduct risk assessments first to justify their needs. Without conducting risk assessments, FAA managers could unnecessarily use resources by installing such equipment in all higher-level air traffic facilities when there may be higher priority needs
- A USDA security specialist decided, despite an ISC baseline requirement that higher-level facilities have X-ray machines, not to recommend an X-ray machine at a higher-level Forest Service facility. The specialist reasoned that unlike other federal buildings with numerous unknown visitors, this facility receives mostly known individuals and a limited number of visitors. The ISC Standard allows for professional judgement; however, the ISC requires that agencies document deviations from the baseline set of countermeasures. Reducing the facility's level of protection without documenting an assessment of risk could result in no record of the basis of the decision for current and future facility managers and security officials to review or use as justification in the case of a question of compliance.

In another case, we found that one higher-level facility did not have access control for employees or visitors nor did it have armed guard patrols.²⁶ The facility manager told us that intelligence and a history without incidents gave leadership reason to believe that these measures were not needed and that therefore the agency did not require and would not fund such protective measures for this facility—in effect, accepting the

²⁶We omitted specific details because the information is considered sensitive.

risks to the facility. Security officials said they also had the same understanding and did not document the matter in the assessment report even though agency policy and the ISC Standard require written documentation when officials deviate from the baseline requirement.

Without security assessments that fully align with the ISC Standard and provide measureable levels of risk, agencies do not have the information they need to determine priorities and make informed resource allocation decisions. For example, they may not be able to assess whether to acquire or forego costly physical-security countermeasures—such as, X-ray machines, access control systems, and closed-circuit television systems—for facilities. Additionally, after determining the need to acquire a countermeasure, agencies must fund the countermeasure. As previously discussed, leading practices in capital decision-making include a comprehensive framework to review, rank, and select from competing project proposals for funding.²⁷ In conducting risk assessments that do not fully align with the ISC Standard (i.e., not assessing threats, vulnerabilities, and consequences and measuring risks), agencies miss the opportunity for more informed funding decisions. Three of the four agencies (CBP, ARS, and the Forest Service) currently prioritize funding for operational needs over physical security needs (see table 2) when agencies’ priorities might be different if they based their decisions on an aligned risk assessment.

Table 2: Selected Agencies Prioritize Operational Needs over Physical Security Needs

Selected agency	How agencies prioritize their needs
U.S. Customs and Border Protection (CBP)	CBP’s real-property maintenance officials said that they typically fund physical security needs within other maintenance, repair, renovation, or capital projects when funding is available. CBP prioritizes operational needs—such as severe life safety-code violations, environmental health issues, and security violations—over physical security countermeasures. Additionally, CBP implements countermeasures when opportunities exist to incorporate them into ongoing facility projects.
Federal Aviation Administration (FAA)	FAA’s Facility Security Risk Management Program Office funds physical security needs at staffed facilities agency-wide. The office prioritizes funding for physical security needs based on criteria such as a facility’s security level, risk data on criminal activity, and whether the facility is “accredited”—that is, met all physical security requirements.
Agricultural Research Service (ARS)	ARS’s facility and regional-level managers prioritize projects based on professional judgment. Regional managers approve projects \$25,000 or less, and headquarters officials review and approve projects costing more than \$25,000. ARS prioritizes life safety projects followed by operational needs, such as repairs to heating or cooling units for employees to work safely, over physical security needs.

²⁷OMB, *Supplement to Circular No. A-11, Part 7, Capital Programming Guide* and [GAO/AIMD-99-32](#).

Selected agency	How agencies prioritize their needs
Forest Service	Forest Service officials in one region said that they evaluate projects with other facility needs based upon professional judgement. They said that they prioritize projects that address operational needs, such as repairing damage caused by a waterline break in an earthquake or structures requiring remediation of bat infestation, over unimplemented projects to address security findings dating to the 2013 assessment.

Source: GAO analysis of agency information. | GAO 18-72

Selected Agencies Reported Facing Challenges in Conducting Security Assessments and Monitoring Results

We found that three of four selected agencies reported facing challenges in conducting physical security assessments at least once every 3 years for higher-level facilities, as required by the ISC Standard, because of competing priorities and resource constraints. Without conducting timely assessments, officials may not have the information they need to properly protect their facilities from risks. We also found that agencies reported facing challenges in monitoring their physical security programs because their policies did not specify data collection or monitoring requirements, as required by *Standards for Internal Control*.²⁸ In addition, without such information, agencies cannot apply capital-planning principals to establish priorities and help agencies make sound capital investment decisions. Three of the four agencies (CBP, ARS, and the Forest Service) did not have an “information system” to track the status of countermeasures, and we found countermeasures were not implemented at all 13 facilities we visited.^{29, 30}

Agencies Have Not Conducted Timely Security Assessments

Standards for Internal Control state that agencies should use quality information on an ongoing basis as a means to monitor program activities and take corrective action, as necessary. The ISC requires that agencies assess higher-level facilities at least once every 3 years—an interval

²⁸[GAO-14-704G](#)

²⁹An “information system” is the people, processes, data, and technology that management organizes to obtain, communicate, or dispose of information.

³⁰We omitted specific details because the information is considered sensitive.

requirement to identify and address evolving risks. We found that three of the four agencies (CBP, ARS, and the Forest Service) did not meet this requirement. Officials reported various challenges including (1) assessments competing with other security activities, (2) an insufficient number of qualified staff to conduct assessments when compared to the number of facilities, or (3) not knowing of the required assessment schedule.

CBP data on assessments from August 2010 to September 2016 shows that the agency had not assessed a significant number of its facilities.³¹ CBP had also not reassessed 10 within the required 3 years, including 6 that had not been reassessed since 2010. CBP security officials attributed the backlog to (1) having too few security specialists assigned to assess about 1,200 facilities and (2) the specialists working on competing priorities, such as revising the security handbook, conducting technical inspections, and reviewing new construction designs and renovation projects. According to CBP security officials, they have developed a plan to eliminate the backlog by the end of fiscal year 2018 by prioritizing the completion of assessments. While we found the plan comprehensive, the schedule did not seem feasible. For example, the plan assumes that one specialist can complete six assessments in 3 consecutive days and that another specialist can complete three assessments in 1 day. In contrast, security officials told us specialists take about 20 work hours (or 2½ days) to conduct an on-site assessment of one facility. CBP officials said that they believe they can meet the time frames of the plan because they have set aside other priorities and have a thorough understanding of the scope of work involved at the facilities. They added that it will not be easy to meet the timeline, but they can accomplish it with a motivated and committed workforce, adequate financial resources, and absent activities that would otherwise require shifting of resources. We question the feasibility of setting aside important priorities, such as updating the policy manual and reviewing physical security elements in new construction designs, as well as the workload assumptions for completing the assessments. Further, these other priorities are also key to securing facilities. Without balancing assessments with competing priorities, CBP's time frames for completing the assessments by the end of fiscal year 2018 may not be feasible and may also result in the agency's not addressing other important physical security responsibilities.

³¹CBP security officials told us that the assessment backlog is greater when counting leased facilities and facilities of all security levels. We omitted specific details because the information is considered sensitive.

Since the ISC issued its standard in 2010, ARS and the Forest Service have assessed their higher-level facilities at least once. However, these agencies have not reassessed all of their higher-level facilities within the 3-year interval requirement. Specifically, security specialists have not conducted required reassessments of two ARS and one Forest Service higher-level facilities.³² The ARS headquarters official explained that the agency had not reassessed the two facilities due to competing priorities and insufficient internal resources. During the course of our review, ARS headquarters officials said they began assessing one of the two ARS facilities in May 2017 and will begin assessing the second facility in October 2017.³³ The Forest Service official explained that the agency missed its security reassessment of the regional office because the facility staff had not requested one. During our visit, facility staff responsible for security told us that they were not aware of the ISC's 3-year interval requirement. Facility staff requested a reassessment, and security officials told us that they expected to complete it by mid-June 2017. Completing this one-time assessment may address the facility's security needs temporarily. However, ARS and the Forest Service have not implemented a long-term schedule with key milestones and lack a means to monitor completion of assessments of higher-level facilities at least once every 3 years. Consequently, these agencies cannot reasonably ensure that they have full knowledge of the risks to their facilities.

FAA data from 2010 through 2016 show that FAA has assessed its 55 higher-level facilities at least once every 3 years.³⁴ FAA policy requires that specialists schedule assessments of higher-level facilities every 12–18 months depending on whether the facility has met FAA physical security standards.

³²According to ARS and Forest Service security officials, USDA security officials conduct about 80 to 85 percent of ARS's physical security assessments and all of Forest Services' assessments, due to limited staffing.

³³In technical comments on the draft sensitive report, USDA said the assessment conducted in May 2017 has been completed. In technical comments on the draft of this report, USDA said the second assessment would be conducted in October 2017.

³⁴After a fire incident at a Chicago facility, a 2015 DOT Inspector General audit found security protocol weaknesses in assessment schedules for the Chicago facility. The report found that FAA had not followed its own policy in conducting a timely security assessment. A subsequent review of that facility found no significant security issues. See U.S. Department of Transportation, *Office of Inspector General Audit Report, FAA's Contingency Plans and Security Protocols Were Insufficient at Chicago Air Traffic Control Facilities*, Report Number: AV-2015-112 (Sept. 29, 2015).

Data Limitations Affect Agencies' Ability to Fully Monitor Security Activities

The ISC Standard states that to make appropriate resource decisions, agencies need information, such as what is being accomplished, what needs management attention, and what is performing at expected levels. We found that agencies' methods of collecting and storing security information had limitations that affected agency and facility officials' oversight of the physical security of their facilities (see table 3).

Table 3: Limitations of Agencies' Information and the Effect on Facility Security

Selected agency	Description and limitation	Effect on facility security
U.S. Customs and Border Protection (CBP)	CBP security officials create a stand-alone electronic spreadsheet of security information—such as assessment schedules and facility security levels—from a real-property inventory database. <i>Limitation:</i> The property database identifies facilities, not specific security needs. In addition, the spreadsheet used to track over 3,600 lines of information has limited use agency-wide.	On an agency-wide level, CBP security officials are not tracking the status of recommended countermeasures. On an ad-hoc basis, we found some facilities in one region have a system for tracking the funding status of countermeasures. ^a
Federal Aviation Administration (FAA)	FAA's agency-wide information system stores security assessments, alerts security managers of upcoming assessments, identifies facility security levels, and monitors the status of recommended countermeasures. ^b <i>Limitation:</i> FAA has not used the security assessment information available in the database to evaluate the cost effectiveness of countermeasures and measure performance.	FAA officials analyze data on an ad-hoc basis, limiting their ability to monitor program activities, take corrective action, and make informed resource decisions.
Agricultural Research Service (ARS)	ARS monitors some security information by facility using a stand-alone electronic document with information, such as names, locations, security levels, and dates of previously completed assessments. <i>Limitation:</i> One individual maintains and tracks this information, limiting its usability agency-wide.	ARS does not have agency-wide information to monitor whether regions or facilities are implementing recommended countermeasures.
Forest Service	The Forest Service does not currently have a means to support monitoring of its physical security at the agency level. <i>Limitation:</i> The Forest Service does not have the ability to store sensitive assessment reports, monitor assessments schedules, or check the status of recommended countermeasures.	Forest Service does not have agency-wide information to monitor whether regions or facilities are scheduling timely assessments or implementing recommended countermeasures.

Source: GAO analysis of agency information. | GAO 18-72

^aTermed the Operational Requirements Based Budgeting Process.

^bThis information system is called the Facility Security Reporting System.

Without having long-term, agency-wide information to monitor whether assessments are conducted on schedule, ARS and the Forest Service may not meet the ISC Standard, resulting in not adequately protecting their facilities and employees.

The ISC Standard also states that agencies should measure their security program's capabilities and effectiveness to demonstrate the need to fund facility security and to make appropriate decisions for allocating resources. However, the agencies in our review were unable to demonstrate appropriate oversight of their physical security programs because:

- CBP's handbook does not include requirements for data collection and analysis for monitoring physical-security program activities. Facility managers and security officials do not enter assessment results, such as the countermeasures recommended for facilities, in the real property database. Consequently, they do not have comprehensive data to manage their security program, assess overall performance, and take any necessary corrective actions. A CBP official told us that a comprehensive database would allow CBP to set priorities for addressing countermeasures. Without including data collection and analysis requirements in its updated handbook, CBP may be unable to monitor the performance of its physical security program.
- FAA's policy does not require ongoing monitoring of physical security information, such as the status of recommended countermeasures or assessment schedules. As a result, FAA officials do not proactively use physical security information to assess the overall performance of its physical security program and take corrective actions before an incident occurs. Without a policy requiring ongoing monitoring of information—an internal control activity, FAA may be unable to assess the overall performance of its security program and take necessary corrective actions.
- USDA has a decentralized security program and places the responsibility on agencies to create their physical security programs. Security officials from ARS and the Forest Service told us that USDA does not have a policy for collecting and managing agency-wide information; however, they said that USDA is drafting a new departmental regulation and manual that will specify (1) the roles and responsibilities of agency and facility managers and (2) electronic-data-reporting requirements for monitoring the performance of the physical security program. USDA officials provided a draft of USDA's regulation and manual for our review. The draft regulation did not

mention data reporting and monitoring, while the draft manual only contained a table of contents that included a section entitled “Facility Tracking Database.” USDA officials expect to issue new policies sometime between October 2017 and April 2018. In the absence of new departmental regulation and manual, USDA and Forest Service officials told us that they have begun to develop a Forest Service system for storing electronic copies of agency-wide assessments and that they plan to expand the use of this system to track site specific assessment dates and status of recommended countermeasures.³⁵ Forest Service officials provided milestone dates and described the capabilities for a future information system, which they expect to complete in September 2017. However, we could not determine whether the manual will have information system requirements to monitor agencies’ physical security program, an internal control activity. Without USDA’s including data collection and analysis requirements in its manual, its agencies may not be able to monitor the performance of their physical security programs.

Selected Agencies Vary in Addressing Recommended Corrective Actions

Without agencies having information to monitor security activities, they were unable to provide us information on the status of countermeasures across their entire portfolio. In order to better understand the status of countermeasures implemented and facilities’ experiences when implementing countermeasures, we determined the status of countermeasures at 13 facilities we visited.

As previously noted, risk management, as it pertains to physical security, involves agency officials monitoring their physical security programs. During our visits to 13 selected facilities, we found the four agencies differed in the number of countermeasures that they had not implemented.³⁶ Facility officials provided us with some information on why countermeasures had not been implemented, specifically:

³⁵In technical comments on the draft sensitive report, USDA said the Forest Service has implemented an ability to store assessment reports.

³⁶We omitted specific details of these countermeasures because the information is considered sensitive.

- CBP had a significant number of recommended countermeasures from 2010 through 2016 that remained open at the eight selected CBP facilities. CBP facility officials gave reasons why recommended countermeasures had not been implemented. At one facility, officials did not know about the recommended countermeasures from its last 2010 assessment because the individuals previously knowledgeable about the assessments left the organization without communicating the results. By taking action to improve facility security, they implemented some needed countermeasures. However, at the time of our review, a large number of the recommendations remained open. At another facility, officials told us that they too had not known (for the same reason mentioned above) of their 2010 assessment, which contained recommended countermeasures. However, these officials told us that they submitted a funding request a few weeks before our visit to address all except one of the open countermeasures.³⁷ In other cases, facilities have not implemented needed countermeasures due to resource constraints or physical site limitations.
- FAA had a large number of recommended countermeasures from 2010 through 2016 that remained open at the time of our review for the two FAA facilities visited. In this case, the most recent security assessment, completed in late 2016, resulted in one facility's having little time to implement countermeasures by the time we conducted our analysis.
- While ARS had closed almost all recommended countermeasures at two facilities at the time of our review, one Forest Service facility had not yet implemented a recommendation (to secure its entrance doors) that was identified in a 2013 security assessment (see bottom center photo, fig. 3). This countermeasure remained open because facility officials said they continued to explore alternatives to address the recommendation.

Figure 3 shows examples of countermeasures not fully implemented at selected facilities we visited.

³⁷Facility officials told us that they will submit the necessary purchase request for the countermeasure for which no funding has yet been requested.

Figure 3: Examples of Recommended Physical Security Countermeasures Not Fully Implemented at Selected Facilities



Armory door has a lever handle lock, but should have a high-security dead bolt lock, access card reader, and intrusion detection device.



Perimeter door has a glass front and lever handle lock; however, it should be made of steel—with a specified thickness—have non-removable hinges, and have a high-security mechanical or electrical lock.



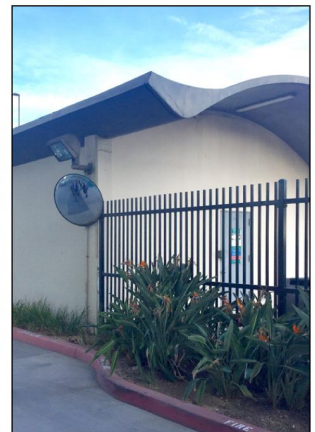
The perimeter door to the biological laboratory should have an exterior door hinge with hinge pins that lock or are welded in place. Exposed door latches should have anti-pick plates installed.



Tree branches growing through the fence have been cut, but the branches hanging over the fence still violate the perimeter-fence clear zone (which sets the distance for which objects must be away from the fence—typically 10 to 20 feet). Cutting the over-hanging branches would help prevent potential intruders from climbing over the fence.



The main entrance door should be attended by a receptionist during business hours and secured at all times. However, the door is left unattended at times and unsecured to allow the general public access.



The perimeter fence clear zone (which sets the distance for which objects must be away from the fence—typically 10 to 20 feet) is violated. However, this violation is not easily corrected as neither the building nor the fence can easily be moved. The land outside of the fence is not federally owned. This situation would require facility managers to weigh and possibly accept the risks.

Source: GAO. | GAO-18-72

During our site visits and discussions with facility staff, we found that physical site limitations or other priorities can make it difficult for facility

managers to implement countermeasures. For example, a countermeasure might involve correcting a clear zone violation—that is, moving an object (such as a brick wall) a certain distance away from the facility’s perimeter fence to prevent a potential intruder from using the object to climb over the fence. However, when the object near the fence is a building and the property outside of the fence is not federally owned (see bottom right photo, fig. 3), it may not be cost effective to correct the clear zone violation. In this situation, the agency bears the responsibility for exploring ways to address the vulnerability. In following the ISC Standard, as previously noted, managers are required to justify and document why they could not implement recommended countermeasures—what the ISC calls risk acceptance.

Conclusions

Selected agencies carry a great responsibility for protecting facilities that support border protection activities, provide safe and efficient air traffic around the country, and protect the quality of the nation’s food supply. With this responsibility comes the need to appropriately assess risk to ensure the security of these agencies’ facilities. However, 7 years after the ISC issued its initial risk-management process standard, each of four selected agencies continued to use assessment methodologies that did not fully align with this standard. During our review, agencies improved their methodologies to better align with the ISC Standard, but the agencies had not yet incorporated the methodologies into their policies and procedures. Without updated policies and procedures requiring a methodology that adheres to the ISC Standard (including all 33 undesirable events now identified in the November 2016 revision to the ISC Standard), agencies may not collect the information needed to assess risk and determine priorities for improved security. This situation could hamper the agencies’ ability to make informed resource allocation decisions or to recommend countermeasures commensurate to the needs at specific facilities. To address challenges in conducting timely assessments, agencies that had a backlog developed plans to address them, but the assumptions used in CBP’s plans and time frames did not appear to fully reflect the agency’s competing priorities and actual experience. Additionally, ARS and Forest Service have not implemented a long-term assessment schedule with key milestones to ensure that higher-level facilities are reassessed at least once every 3 years. Further, in cases where the agencies may have had risk assessment information, CBP, ARS, and the Forest Service lack the means to collect, store, and analyze this information in order to monitor the status of a facility’s

security. Without these key aspects of a comprehensive security program—a methodology that meets the standard, policies, and procedures that incorporate that methodology; the ability to complete assessments on time; and information to perform monitoring—agencies remain vulnerable to substantial security risks.

Recommendations for Executive Action

To improve agencies' physical security programs' alignment with the ISC *Risk Management Process for Federal Facilities* and *Standards for Internal Control in the Federal Government* for information and monitoring, we recommend that the

Commissioner of U.S. Customs and Border Protection take the following three actions:

- with regard to the updated *Security Policy and Procedures Handbook*, include:
 - the ISC's *Risk Management Process for Federal Facilities* requirement to assess all undesirable events, consider all three factors of risk, and document deviations from the standard, and
 - data collection and analysis requirements for monitoring the performance of CBP's physical security program.
- revise the assumptions used in the plan to address the backlog to balance assessments with competing priorities, such as updating the policy manual and reviewing new construction design, to develop a feasible time frame for completing the assessment backlog.

Secretary of Transportation direct the FAA Administrator to take the following three actions:

- develop a plan that provides sufficient details on the activities needed and time frames within the date when FAA will implement an improved methodology;
- update FAA's policy to require the use of a methodology that fully aligns with the ISC's *Risk Management Process for Federal Facilities* for assessing all undesirable events, considering all three factors of risk, and documenting all deviations from the standard countermeasures; and

-
- update FAA's policy to include ongoing monitoring of physical security information.

Secretary of Agriculture take the following two actions:

- include data collection and analysis requirements for monitoring the performance of agencies' physical security programs, in the department's revised physical-security manual, and
- direct the Administrator of the Agricultural Research Service and the Chief of the Forest Service to
 - implement and monitor a long-term assessment schedule with key milestones to ensure that higher-level facilities are reassessed at least once every 3 years.

Agency Comments

We provided a draft of this report to the Departments of Homeland Security, Transportation, and Agriculture for review and comment. All three departments agreed with the findings and recommendations for their respective agencies. DHS agreed with our recommendations and provided actions and timeframes for completion. With regard to our recommendation to update the *Security Policy and Procedures Handbook*, DHS stated that CBP is updating the handbook to include: (1) a discussion and diagram of the ISC risk management process and its application within CBP's assessment processes; (2) specific guidance for conducting risk assessments in accordance with the ISC's *Risk Management Process for Federal Facilities*; and (3) a requirement and guidance for data collection and analysis in support of a robust physical security program. With regard to our recommendation to revise the assumptions used in the plan to address the assessment backlog, DHS stated that CBP has reevaluated current priorities and believes the current plan to eliminate the risk assessment backlog by the end of fiscal year 2018 is achievable. DHS also provided technical comments, which we incorporated as appropriate. DHS's official written response is reprinted in appendix IV.

DOT also agreed with our recommendations and by e-mail requested that we publish the response to the sensitive version of this report. DOT stated that FAA continues to refine its policy and develop processes that address the ISC threats, vulnerabilities, and consequences. Further, DOT stated that FAA would either validate that current mitigation strategies

address those risks or apply additional appropriate countermeasures. DOT stated that it will provide a detailed response to each recommendation within 60 days from the date of this report. DOT's official written response is reprinted in appendix V.

USDA agreed with our recommendations and provided the agency-wide actions for completion. USDA provided a plan to ensure compliance with the ISC's *Risk Management Process for Federal Facilities* by development of a standard physical-security assessment process and by initiation of a compliance program to track assessments and monitor the installation of countermeasures. In an e-mail, USDA provided milestone dates and planned completion by January 2019. USDA's official written response is reprinted in appendix VI.

If you or your staff has any questions about this report, please contact me at (202) 512-2834 or RectanusL@gao.gov. GAO staff who made key contributions to this report are listed in appendix VI.

A handwritten signature in black ink that reads "Lori Rectanus". The signature is written in a cursive, flowing style.

Lori Rectanus
Director, Physical Infrastructure

Appendix I: Objectives, Scope, and Methodology

This report examines: (1) how selected agencies' assessment methodologies align with the Interagency Security Committee's (ISC) risk management standard for identifying necessary countermeasures and (2) what management challenges, if any, selected agencies reported facing in conducting physical security assessments and monitoring the results.

To determine how selected agencies' assessment methodologies align with ISC standards for identifying the necessary countermeasures, we identified federal executive branch departments and agencies reported by the Department of Homeland Security (DHS) to have received delegations of authority to protect their own buildings.¹ We reviewed the Federal Real Property Council's data on the Federal Real Property Profile to identify federally owned and agency-controlled buildings.² We determined that these data were sufficiently reliable for the purpose of our reporting objectives based upon our recent report that reviewed these data fields.³ We selected four agencies based upon their large quantity of reported federally owned and agency-controlled buildings: DHS, U.S. Customs and Border Protection (CBP); Department of Transportation (DOT), Federal Aviation Administration (FAA); United States Department of Agriculture (USDA), Agricultural Research Service (ARS) and USDA's United States Forest Service (Forest Service). This methodology purposely does not include federal buildings protected by FPS and under the control of the General Services Administration as well as other

¹These delegations of authority allow other federal departments and agencies to provide law enforcement and/or contract guard services under DHS's authority pursuant to 40 U.S.C. § 1315 note. FPS, *Interim Delegation Assessment Plan* (Washington, D. C.: November 2012).

²Specified civilian federal executive agencies and departments subject to the Chief Financial Officers Act of 1990 are annually required to submit real property data at the constructed asset level to the Federal Real Property Profile database pursuant to Executive Order 13327.

³GAO, Federal Real Property: Improving Data Transparency and Expanding the National Strategy Could Help Address Long-standing Challenges, [GAO-16-275](#) (Washington: D.C.: Mar. 31, 2016).

agencies that we reported on in our previous work.⁴ We obtained and reviewed one particular ISC standard, *The Risk Management Process for Federal Facilities* (the ISC Standard) and its related appendices for assessing physical security and providing recommended countermeasures at federal facilities.⁵ We obtained and analyzed the selected departments' and agencies' facility-security policies and procedures for a risk assessment methodology. According to the ISC Standard, agencies' risk assessment methodologies must:

- consider all of the undesirable events identified in the ISC Standard as possible risks to federal facilities as listed in appendix III;⁶
- assess the threat, consequences, and vulnerability to specific undesirable events;
- produce similar or identical results when applied by various security professionals; and
- provide sufficient justification for deviations from the ISC-defined security baseline.

We limited the scope of this review to the first two standards above because agencies' adherence to these standards could be objectively verified by reviewing and analyzing agency documentation and interviewing agency officials, and their adherence to the two additional standards could not be verified in this manner. We did not conduct risk assessments with independent security professionals to evaluate: 1) the results from prior agency evaluations and 2) the sufficiency of

⁴GAO, *Federal Facility Security: Additional Actions Needed to Help Agencies Comply with Risk Assessment Methodology Standards*, [GAO-14-86](#) (Washington, D. C.: Mar. 5, 2014); GAO, *Homeland Security: Action Needed to Better Assess Cost-Effectiveness of Security Enhancements at Federal Facilities*, [GAO-15-444](#) (Washington, D. C.: Mar. 24, 2015); and GAO, *Homeland Security: Actions Needed to Better Manage Security Screening at Federal Buildings and Courthouses*, [GAO-15-445](#) (Washington, D. C.: Mar. 31, 2015)

⁵ISC, *The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard* (Washington, D. C.: November 2016). The ISC Standard incorporates the following appendixes: "Appendix A: The Design-Basis Threat Report;" "Appendix B: Countermeasures;" and "Appendix C: Child-Care Center Level of Protection Template."

⁶According to ISC officials, the term "consider" means that as a starting point or baseline, an agency's methodology must include all of the undesirable events listed in the ISC Standard. However, agencies have the flexibility to omit events they determine are not applicable to their facilities (or a particular facility) and/or add events that are not included in the ISC Standard as long as agencies document any omission.

justifications for deviations from the ISC-defined security baseline, as both evaluations were outside of the scope of the engagement. Therefore, for the purposes of this report, risk assessment policies, procedures and resulting methodology that align with ISC standards are those that consider all of the undesirable events and assess the threats, consequences, and vulnerabilities to specific undesirable events. We reviewed and analyzed information to answer the following five questions:

1. Do the policies and procedures mention the ISC standards?
2. Do the policies and procedures consider all of the undesirable events?
3. Do the policies and procedures assess the threat of specific undesirable events?
4. Do the policies and procedures assess the consequences of specific undesirable events?
5. Do the policies and procedures assess the vulnerability to specific undesirable events?

We answered each of these questions as either a “Yes” or “No” for our selected agencies. The “No” answer to questions 3, 4, and 5 includes the following two possibilities: (a) the agency’s threat, consequence, or vulnerability ratings are not tied to specific undesirable events, or (b) the agency does not have a framework or formalized steps within which it collects and analyzes threat-, consequence-, or vulnerability-related information. If the answer to each of the five questions was “Yes,” then the agency’s overall risk assessment methodology aligns with ISC risk assessment standards for the purposes of this report. If the answer to one or more of the five questions was “No,” then the agency’s methodology does not align with ISC standards for the purposes of this report.

We interviewed security officials at ISC; three departments (DHS, DOT, and USDA); and four agencies (CBP, FAA, ARS, and the Forest Service). We obtained and analyzed agency guidance on prioritizing physical security needs and interviewed agencies’ facility maintenance and budget officials. We reviewed the ISC’s best practices for planning for physical security resources within an agency budget process.⁷ Additionally, we reviewed the Office of Management and Budget’s and our leading

⁷ISC, Best Practices for Planning and Managing Physical Security Resources: An Interagency Security Committee Guide (Washington, D. C.: December 2015).

practices in capital decision-making that provide agencies with guidance for prioritizing budget decisions such as “countermeasure projects.”⁸ We also reviewed *Standards for Internal Control in the Federal Government* because internal controls play a significant role in helping agencies achieve their mission-related responsibilities.⁹ Our findings from our review of the selected agencies are not generalizable to all ISC member agencies, but provide insight into and illustrative examples about selected agencies’ facility risk-assessment methodologies.

To determine what management challenges selected agencies reported facing in conducting physical security assessments and monitoring results, we interviewed agencies’ security, maintenance, and budget officials. We requested agency security officials to provide portfolio- wide data on facility security assessments for our review in order to select sites to visit and analyze data for dates of assessments and the status of findings. We assessed the reliability of this data through interviews with knowledgeable agency staff and a review for completeness and any unexpected values. We compiled information from physical security assessments when no portfolio-wide agency data were available. We determined that these data were sufficient for the purpose of our reporting objectives and selected geographically dispersed sites with buildings with higher reported security levels per the ISC Standard, as these higher security levels have greater requirements and therefore the potential for greater resource needs. See appendix II for the 13 sites we selected. For these selected sites, we interviewed agency staff concerning the assessment process, site-specific findings, recommendations, justification for deviations from ISC’s baseline standards, and management challenges faced in addressing physical security needs. We observed and photographed the status of the findings from the site physical security assessments. We did not independently determine what constitutes a management challenge or a physical security finding. Rather, we relied on these stakeholders to determine these physical security concerns as defined in their own standards and guidance. The information from our selected sites is illustrative and cannot be generalized to sites agency-wide.

⁸According to leading practices established by OMB and GAO: Office of Management and Budget, Supplement to *Circular No. A-11, Part 7, Capital Programming Guide* (Washington, D.C.: July 2016) and GAO, *Executive Guide: Leading Practices in Capital Decision-Making*, [GAO/AIMD-99-32](#) (Washington, D.C.: December 1998).

⁹GAO, *Standards for Internal Control in the Federal Government*, [GAO-14-704G](#) (Washington, D. C.: September 2014).

The performance audit upon which this report is based was conducted from June 2016 to August 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 subsequently worked with DHS, DOT and USDA from August 2017 to October 2017 to prepare this version of the original report for public release. This public version was also prepared in accordance with these standards.

Appendix II: Selected Facilities GAO Visited

Table 4: 13 Facilities GAO Visited at the Department of Homeland Security (DHS), U.S. Customs and Border Protection (CBP); Department of Transportation (DOT), Federal Aviation Administration (FAA); and the United States Department of Agriculture (USDA), Agricultural Research Service (ARS) and the Forest Service

Department	Agency	Facility ^a	Facility Security Level ^b
DHS	CBP	1	IV
DHS	CBP	2	III
DHS	CBP	3	IV
DHS	CBP	4	III
DHS	CBP	5	IV
DHS	CBP	6	III
DHS	CBP	7	III
DHS	CBP	8	III
DOT	FAA	9	III
DOT	FAA	10	III
USDA	ARS	11	III
USDA	ARS	12	IV
USDA	Forest Service	13	III

Source: GAO selected sites visited. | GAO 18-72

^aWe omitted specific details of these domestic facilities because the information is considered sensitive.

^bFacility security level, ranging from level I (lowest risk) for the least critical facilities and generally having 100 or fewer employees to level V (highest risk) for the most critical facilities and generally having greater than 750 employees. The facility security level designation determines the facility's baseline countermeasures.

Appendix III: The Interagency Security Committee's Undesirable Events

Table 5: The Interagency Security Committee's Undesirable Events

Undesirable event ^a
1. Aircraft as a Weapon
2. Arson
3. Assault
4. Ballistic Attack – Active Shooter
5. Ballistic Attack – Small Arms
6. Ballistic Attack – Standoff Weapons
7. Breach of Access Control Point – Covert
8. Breach of Access Control Point – Overt
9. Chemical/Biological/Radiological (CBR) Release – External
10. Chemical/Biological/Radiological (CBR) Release – Internal
11. Chemical/Biological/Radiological (CBR) Release – Mail or Delivery
12. Chemical/Biological/Radiological (CBR) Release – Water Supply
13. Civil Disturbance
14. Disruption of Facility or Security Systems
15. Explosive Device – Man-Portable External
16. Explosive Device – Man-Portable Internal
17. Explosive Device – Suicide/Homicide Bomber
18. Explosive Device – Vehicle Borne Improvised Explosive Device
19. Explosive Device – Mail or Delivery
20. Hostile Surveillance
21. Insider Threat
22. Kidnapping
23. Release of Onsite Hazardous Materials
24. Robbery
25. Theft
26. Unauthorized Entry – Forced
27. Unauthorized Entry – Surreptitious
28. Vandalism
29. Vehicle Ramming

**Appendix III: The Interagency Security
Committee's Undesirable Events**

Undesirable event^a
30. Workplace Violence
31. Unauthorized Access
32. Interruption of Services
33. Modification of Services

Source: ISC, The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard (Washington, D. C.: November 2016). | GAO 18-72

^aWe omitted specific descriptions of these undesirable events because the information is considered sensitive

Appendix IV: Comments from the Department of Homeland Security

U.S. Department of Homeland Security
Washington, DC 20528



**Homeland
Security**

October 11, 2017

Lori Rectanus
Director, Physical Infrastructure
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Re: Management's Response to Draft Report GAO-18-72, "FEDERAL FACILITY
SECURITY: Selected Agencies Should Improve Methods for Assessing and Monitoring
Risk"

Dear Ms. Rectanus:

Thank you for the opportunity to review and comment on this draft report. The U.S. Department of Homeland Security (DHS) appreciates the U.S. Government Accountability Office's (GAO) work in planning and conducting its review and issuing this report.

With more than 1,200 facilities and 60,000 personnel to protect, U.S. Customs and Border Protection's (CBP) organizational security missions, physical and otherwise, continue to be an integral element of day-to-day operations. CBP recognizes the importance of allocating sufficient resources to these missions and has taken numerous steps to effectively manage its expansive security portfolio. For example, CBP is committed to establishing a mature Security Liaison program, conducting Physical Security Vulnerability Assessments at Facility Security Level III, IV, and V facilities, and managing support for the entire construction design and build cycle for new and renovated facilities. In addition, CBP is taking steps to ensure all periodic risk assessments comply with Interagency Security Committee (ISC) standards.

The draft report contains three recommendations with which the Department concurs. Attached find our detailed response to each of the recommendations.

Again, thank you for the opportunity to review and comment on this draft report. Technical comments were previously provided under separate cover. Please feel free to contact me if you have any questions. We look forward to working with you in the future.

Sincerely,

A handwritten signature in black ink, appearing to read "Jim H. Crumacker".

JIM H. CRUMACKER, CIA, CFE
Director
Departmental GAO-OIG Liaison Office

Attachment

**Attachment: DHS Management Response to Recommendations Contained in
GAO-18-72**

GAO recommended that the Commissioner of U.S. Customs and Border Protection:

Recommendation 1: Update the Security Policy and Procedures Handbook to include the Interagency Security Committee's (ISC's) Risk Management Process for Federal Facilities Standard to assess all undesirable events, consider all three factors of risk, and document deviations from the standard.

Response: Concur. The Office of Professional Responsibility (OPR) is currently engaged in updating CBP physical security policy and procedures and will issue them under the CBP Physical Security Policies and Procedures Handbook (PSPPH). The handbook will include a discussion and diagram of the ISC's Risk Management Process and its application within CBP's facility procurement, construction design, and assessment processes.

OPR has drafted a chapter in the PSPPH dedicated to risk informed decision-making. This chapter provides the explanation and guidance for conducting local risk assessments, identifying the ISC requirement for the three- and five-year periodic assessments, and the five-step process for making sound risk-related decisions. This includes identifying and assessing the threat, developing controls, implementing controls, and supervising, evaluating, and defining how these relate to the Designated Official. The chapter ties this information into the ISC Risk Management Process flowchart and illustrates how CBP transitions from the Federal Security Level determination to identifying and assessing risks then determining if the level of protection is commensurate with risks. The chapter concludes with the application of risk management to the various property types (e.g., new construction, modernization, leased, or free space) encountered within the CBP facility inventory.

The core of the PSPPH update is the physical security of federal facilities; however, the handbook also identifies the roles and responsibilities that other CBP offices have in the agency's overall physical security posture and OPR will work with these offices in assessing overall threats. Estimated interim milestones:

- March 31, 2018 OPR will develop the draft PSPPH.
- September 30, 2018 OPR will disseminate the draft PSPPH for agency-wide review and comment.
- June 30, 2019 Publish the final, signed revision of the PSPPH.

The overall ECD is June 30, 2019.

Recommendation 2: Update the Security Policy and Procedures Handbook to include data collection and analysis requirements for monitoring the performance of its physical security program.

Response: Concur. In reference to monitoring physical security program performance, OPR acknowledges the requirement and the importance for the updated PSPPH to include data collection and analysis in support of a robust physical security program. The ISC's Risk Management Process for Federal Facilities Standard will be used extensively as a primary source document for this topic. The PSPPH will include guidance on collecting and analyzing data that will provide meaningful support for addressing the physical security of agency employees, the protection of agency assets, (both information and physical), and compliance with federal standards.

As previously noted in recommendation 1, OPR's risk informed decision-making chapter in the PSPPH includes the important process of supervising and evaluating the implementation of controls. In addition to ensuring that the standards are enforced, it also provides the means to validate the adequacy of control measures, and the ability to identify strengths or weaknesses and make changes accordingly. Further, the draft PSPPH also contains a chapter dedicated to physical security performance measures. This chapter includes such information as the ISC policy for performance measures and the value of performance measures to resource allocation, as well as the effectiveness of control measures. The ISC's Risk Management process for Federal Facilities Standard was the primary source document for this topic. Estimated interim milestones:

- March 31, 2018 OPR will develop the draft PSPPH.
- September 30, 2018 OPR will disseminate the draft PSPPH for agency-wide review and comment.
- June 30, 2019 Publish the final, signed revision of the PSPPH.

The overall ECD is June 30, 2019.

Recommendation 3: Revise the plan's [plan to eliminate the backlog of facility risk assessments] assumptions to balance assessments with competing priorities, such as updating the policy manual and reviewing new construction design, to develop a feasible time frame for completing the assessment backlog.

Response: Concur. CBP acknowledges that planning for the assessment of all CBP-owned facilities requires an aggressive approach that includes balancing other OPR requirements, such as policy development, construction design, assessment of other CBP-occupied properties, and special certification programs. That said, CBP has reevaluated current priorities and believes the current plan to eliminate the risk assessment backlog is achievable. Moreover, CBP security personnel who have developed an expertise in reviewing the facilities within their respective Areas of Responsibility were consulted during the development of the plan and are confident in their ability to meet the established timeline.

At the end of Fiscal Year (FY) 2017, OPR completed 113 assessments of CBP-owned facilities, which exceeds the targeted number of 103 for Fiscal Year (FY) 2017. When added to the FY 2015 and FY 2016 subtotals, this equates to 202 assessments of the 240 CBP-owned facilities, or 84 percent compliance with the ISC's periodic risk assessment standard. CBP will complete the remaining unassessed CBP-owned facilities in FY 2018 for 100 percent ISC risk assessment

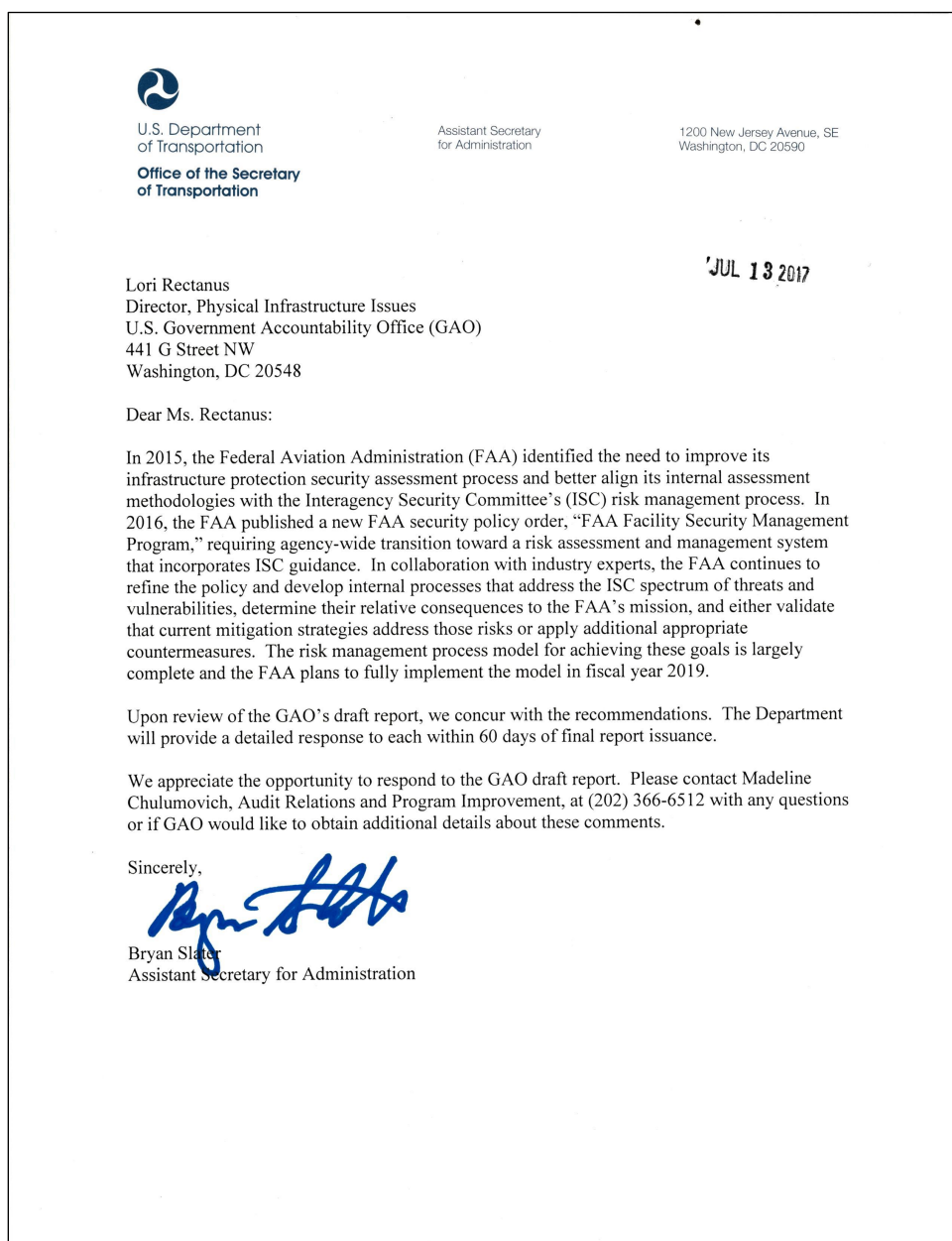
compliance. This milestone then marks the point when CBP will initiate a predictable assessment cycle to sustain ISC compliance. Estimated interim milestones:

- June 30, 2018 OPR will complete assessments for 90 percent of the current CBP-owned facilities.
- July 31, 2018 OPR will conduct a reassessment of the plan for reducing the backlog of Risk Assessments and update, as needed.
- September 30, 2018 OPR will eliminate the assessment backlog and achieve a recurring cyclical assessment review schedule in-line with the ISC standards.

The overall ECD is September 30, 2018

Error! No text of specified style in document.

Appendix V: Comments from the Department of Transportation



Appendix VI: Comments from the Department of Agriculture




United States
Department of
Agriculture

Office of Homeland
Security and
Emergency
Coordination

1400 Independence
Avenue SW
Washington, DC
20250

TO: Lori Rectanus
Director, Physical Infrastructure
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

FROM: Josh Bornstein  **OCT 10 2017**
Acting Director,
Office of Homeland Security and Emergency Coordination

SUBJECT: Response to Report GAO 102257, "Federal Facility Security: Agencies
Should Improve Methods for Assessing and Monitoring Risk."

Thank you for the opportunity to review the subject report and provide the U.S. Government Accountability Office (GAO) with the steps the U.S. Department of Agriculture (USDA) is taking to address the listed recommendations. The USDA appreciates GAO's work in planning and conducting its review and issuing this report. The subject report contained two recommendations with which the Department concurs.

USDA takes the mission seriously to provide leadership on food, agriculture, natural resources, rural development, nutrition, and related issues. We must also strive to protect the public, our workforce, assets, and facilities. Therefore, USDA has formulated a plan to ensure our agencies and offices are compliant with Interagency Security Committee (ISC) Standards. Our way forward consists of three lines of effort to include development of physical security policies and procedures, development of a standard physical security assessment process that is compliant with the ISC Risk Management Process, and initiation of a compliance program to track assessments and monitor installation of countermeasures.

Again, thank you for the opportunity to review and comment on this report. Please feel free to contact me if you have any questions. We look forward to working with you in the future.

Appendix VII: GAO Contact and Staff Acknowledgments

GAO Contact

Lori Rectanus, 202-512-2834, rectanusl@gao.gov

Staff Acknowledgments

In addition to the contact named above, Amelia Shachoy (Assistant Director), Steve Martinez (Analyst-in-Charge), Jennifer Clayborne, George Depaoli, Geoffrey Hamilton, Joshua Ormond, Alison Snyder, Amelia Michelle Weathers, and Elizabeth Wood made key contributions to this report.

Appendix VIII: Accessible Data

Agency Comment Letters

Text of Appendix IV: Comments from the Department of Homeland Security

October 11, 2017

Lori Rectanus

Director, Physical Infrastructure

U.S. Government Accountability Office 441 G Street, NW

Washington, DC 20548

Re: Management's Response to Draft Report GAO-18-72, "FEDERAL FACILITY SECURITY: Selected Agencies Should Improve Methods for Assessing and Monitoring Risk"

Dear Ms. Rectanus:

Thank you for the opportunity to review and comment on this draft report. The U.S. Department of Homeland Security (DHS) appreciates the U.S. Government Accountability Office's (GAO) work in planning and conducting its review and issuing this report.

With more than 1,200 facilities and 60,000 personnel to protect, U.S. Customs and Border Protection's (CBP) organizational security missions, physical and otherwise, continue to be an integral element of day-to-day operations. CBP recognizes the importance of allocating sufficient resources to these missions and has taken numerous steps to effectively manage its expansive security portfolio. For example, CBP is committed to establishing a mature Security Liaison program, conducting Physical Security Vulnerability Assessments at Facility Security Level III, IV, and V facilities, and managing support for the entire construction design and build cycle for new and renovated facilities. In addition, CBP is taking steps to ensure all periodic risk assessments comply with Interagency Security Committee (ISC) standards.

The draft report contains three recommendations with which the Department concurs. Attached find our detailed response to each of the recommendations.

Again, thank you for the opportunity to review and comment on this draft report. Technical comments were previously provided under separate cover. Please feel free to contact me if you have any questions. We look forward to working with you in the future.

Jim H. Crumpacker Director

Departmental GAO-OIG Liaison Office

Attachment

Attachment: DHS Management Response to Recommendations
Contained in GA0-18-72

GAO recommended that the Commissioner of U.S. Customs and Border Protection:

Recommendation 1: Update the Security Policy and Procedures Handbook to include the Interagency Security Committee's (JSC's) Risk Management Process for Federal Facilities Standard to assess all undesirable events, consider all three factors of risk, and document deviations from the standard.

Response: Concur.

The Office of Professional Responsibility (OPR) is currently engaged in updating CBP physical security policy and procedures and will issue them under the CBP Physical Security Policies and Procedures Handbook (PSPPH). The handbook will include a discussion and diagram of the JSC's Risk Management Process and its application within CBP's facility procurement, construction design, and assessment processes.

OPR has drafted a chapter in the PSPPH dedicated to risk informed decision-making. This chapter provides the explanation and guidance for conducting local risk assessments, identifying the ISC requirement for the three- and five-year periodic assessments, and the five-step process for making sound risk-related decisions. This includes identifying and assessing the threat, developing controls, implementing controls, and supervising, evaluating, and defining how these relate to the Designated

Official. The chapter ties this information into the JSC Risk Management Process flowchart and illustrates how CBP transitions from the Federal Security Level determination to identifying and assessing risks then determining if the level of protection is commensurate with risks. The chapter concludes with the application of risk management to the various property types (e.g., new construction, modernization, leased, or free space) encountered within the CBP facility inventory.

The core of the PSPPH update is the physical security of federal facilities; however, the handbook also identifies the roles and responsibilities that other CBP offices have in the agency's overall physical security posture and OPR will work with these offices in assessing overall threats.

Estimated interim milestones:

- March 31, 2018 - OPR will develop the draft PSPPH.
- September 30, 2018 - OPR will develop the draft PSPPH.
- June 30, 2019 OPR will develop the draft PSPPH.

OPR will disseminate the draft PSPPH for agency-wide review and comment.

Publish the final, signed revision of the PSPPH.

The overall ECO is June 30, 2019.

Recommendation 2: Update the Security Policy and Procedures Handbook to include data collection and analysis requirements for monitoring the performance of its physical security program.

Response: Concur.

In reference to monitoring physical security program performance, OPR acknowledges the requirement and the importance for the updated PSPPH to include data collection and analysis in support of a robust physical security program. The ISC's Risk Management Process for Federal Facilities Standard will be used extensively as a primary source document for this topic. The PSPPH will include guidance on collecting and analyzing data that will provide meaningful support for addressing the physical security of agency employees, the protection of agency assets, (both information and physical), and compliance with federal standards.

As previously noted in recommendation 1, OPR's risk informed decision-making chapter in the PSPPH includes the important process of supervising and evaluating the implementation of controls. In addition to ensuring that the standards are enforced, it also provides the means to validate the adequacy of control measures, and the ability to identify strengths or weaknesses and make changes accordingly. Further, the draft PSPPH also contains a chapter dedicated to physical security performance measures. This chapter includes such information as the ISC policy for performance measures and the value of performance measures to resource allocation, as well as the effectiveness of control measures. The ISC's Risk Management process for Federal Facilities Standard was the primary source document for this topic.

Estimated interim milestones:

- March 31, 2018 - OPR will develop the draft PSPPH.
- September 30, 2018 - OPR will disseminate the draft PSPPH for agency-wide review and comment.
- June 30, 2019 - Publish the final, signed revision of the PSPPH.

The overall ECD is June 30, 2019.

Recommendation 3: Revise the plan's [plan to eliminate the backlog of facility risk assessments] assumptions to balance assessments with competing priorities, such as updating the policy manual and reviewing new construction design, to develop a feasible time frame for completing the assessment backlog.

Response: Concur.

CBP acknowledges that planning for the assessment of all CBP-owned facilities requires an aggressive approach that includes balancing other OPR requirements, such as policy development, construction design, assessment of other CBP-occupied properties, and special certification programs. That said, CBP has reevaluated current priorities and believes the current plan to eliminate the risk assessment backlog is achievable. Moreover, CBP security personnel who have developed an expertise in reviewing the facilities within their respective Areas of Responsibility were consulted during the development of the plan and are confident in their ability to meet the established timeline.

At the end of Fiscal Year (FY) 2017, OPR completed 113 assessments of CBP-owned facilities, which exceeds the targeted number of 103 for

Fiscal Year (FY) 2017. When added to the FY 2015 and FY 2016 subtotals, this equates to 202 assessments of the 240 CBP-owned facilities, or 84 percent compliance with the ISC's periodic risk assessment standard. CBP will complete the remaining unassessed CBP-owned facilities in FY 2018 for 100 percent JSC risk assessment compliance. This milestone then marks the point when CBP will initiate a predictable assessment cycle to sustain ISC compliance. Estimated interim milestones:

- June 30, 2018 - OPR will complete assessments for 90 percent of the current CBP-owned facilities.
- July 31, 2018 - OPR will conduct a reassessment of the plan for reducing the backlog of Risk Assessments and update, as needed.
- September 30, 2018 - OPR will eliminate the assessment backlog and achieve a recurring cyclical assessment review schedule in-line with the ISC standards.

The overall ECD is September 30, 2018

Text of Appendix V: Comments from the Department of Transportation

Lori Rectanus

Director, Physical Infrastructure Issues

U.S. Government Accountability Office (GAO)

441 G Street NW Washington, DC 20548

Dear Ms. Rectanus:

In 2015, the Federal Aviation Administration (FAA) identified the need to improve its infrastructure protection security assessment process and better align its internal assessment methodologies with the Interagency Security Committee's (ISC) risk management process. In 2016, the FAA published a new FAA security policy order, "FAA Facility Security Management Program," requiring agency-wide transition toward a risk assessment and management system that incorporates ISC guidance. In collaboration with industry experts, the FAA continues to refine the policy and develop internal processes that address the ISC spectrum of threats and vulnerabilities, determine their relative consequences to the FAA's

mission, and either validate that current mitigation strategies address those risks or apply additional appropriate countermeasures. The risk management process model for achieving these goals is largely complete and the FAA plans to fully implement the model in fiscal year 2019.

Upon review of the GAO's draft report, we concur with the recommendations. The Department will provide a detailed response to each within 60 days of final report issuance.

We appreciate the opportunity to respond to the GAO draft report. Please contact Madeline Chulumovich, Audit Relations and Program Improvement, at (202) 366-6512 with any questions or if GAO would like to obtain additional details about these comments.

Sincerely

Bryan Slater

Assistant Secretary for Administration

Text of Appendix VI: Comments from the Department of Agriculture

Lori Rectanus

Director, Physical Infrastructure

U.S. Government Accountability Office 441 G Street, NW

Washington, DC 20548

FROM: Josh Bornstein Acting Director,

SUBJECT: Response to Report GAO 102257, "Federal Facility Security: Agencies Should Improve Methods for Assessing and Monitoring Risk."

Thank you for the opportunity to review the subject report and provide the U.S. Government Accountability Office (GAO) with the steps the U.S. Department of Agriculture (USDA) is taking to address the listed recommendations. The USDA appreciates GAO's work in planning and conducting its review and issuing this report. The subject report contained two recommendations with which the Department concurs.

USDA takes the mission seriously to provide leadership on food, agriculture, natural resources, rural development, nutrition, and related issues. We must also strive to protect the public, our workforce, assets, and facilities. Therefore, USDA has formulated a plan to ensure our agencies and offices are compliant with Interagency Security Committee (ISC) Standards. Our way forward consists of three lines of effort to include development of physical security policies and procedures, development of a standard physical security assessment process that is compliant with the ISC Risk Management Process, and initiation of a compliance program to track assessments and monitor installation of countermeasures.

Again, thank you for the opportunity to review and comment on this report. Please feel free to contact me if you have any questions. We look forward to working with you in the future.

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