United States Government Accountability Office

Report to the Chairman, Subcommittee on Oversight and Management Efficiency, Committee on Homeland Security, House of Representatives

March 2014

FEDERAL FACILITY SECURITY

Additional Actions Needed to Help Agencies Comply with Risk Assessment Methodology Standards

GAO-14-86

March 2014

FEDERAL FACILITY SECURITY

Additional Actions Needed to Help Agencies Comply With Risk Assessment Methodology Standards

GAO Highlights

Highlights of GAO-14-86, a report to the Chairman, Subcommittee on Oversight and Management Efficiency, Committee on Homeland Security, House of Representatives

Why GAO Did This Study

The 2012 shooting at the Anderson Federal Building in Long Beach, California, demonstrates that federal facilities and their employees as well as the public who visit federal buildings continue to be the targets of violence. The Federal Protective Service and about 30 other federal agencies are responsible for protecting civilian federal facilities and their occupants from potential threats, in part, by assessing risks to their facilities. ISC—an interagency organization led by the Department of Homeland Security— issues standards for facility protection.

GAO was asked to examine how federal agencies assess risk to their facilities. This report assesses (1) the extent to which selected ISC member agencies' facility risk assessment methodologies align with ISC's risk assessment standards, and (2) how ISC assists member agencies in developing risk assessment methodologies and monitors compliance with these standards. GAO selected 9 of 53 ISC member agencies based on their missions and number of facilities. GAO compared each selected agency's risk assessment methodology to ISC's risk assessment standards. ISC is required to enhance security in and protection of federal facilities government-wide; recommendations GAO makes are to ISC and not its member agencies.

What GAO Recommends

GAO recommends that ISC take action to assess member agencies' compliance and provide additional risk-assessment methodology guidance. DHS concurred with GAO's recommendations.

View GAO-14-86. For more information, contact Mark L. Goldstein at (202) 512-2834 or goldsteinm@gao.gov.

What GAO Found

Three of the nine selected agencies' risk assessment methodologies that GAO reviewed—the Department of Energy (DOE), the Department of Justice (DOJ), and the Department of State (State)—fully align with the Interagency Security Committee's (ISC) risk assessment standards, but six do not—the Department of the Interior (DOI), the Department of Veterans Affairs (VA), the Federal Protective Service (FPS), the Federal Emergency Management Agency (FEMA), the Nuclear Regulatory Commission (NRC), and the Office of Personnel Management (OPM). As a result, these six agencies may not have a complete understanding of the risks facing approximately 52,000 federal facilities and may be less able to allocate security resources cost-effectively at the individual facility level or across the agencies' facility portfolios. ISC's *The Risk Management Process for Federal Facilities* (*RMP*) standard requires that agencies' facility risk assessment methodologies must (1) consider all of the undesirable events identified in the *RMP* as possible risks to federal facilities, and (2) assess the threat, consequences, and vulnerability to specific undesirable events. Six of the nine agencies' methodologies GAO reviewed do not align with ISC's standards because the methodologies do not (1) consider all of the undesirable events in the *RMP* or (2) assess threat, consequences, or vulnerability to specific undesirable events. For example, five agencies (DOI, VA, FEMA, FPS, and NRC), do not assess the threat, consequences, or vulnerability to specific undesirable events, as ISC requires. The reasons why varied; for example, VA said that its methodology was in place before ISC issued its standards. Officials from that agency told us they were working to update their methodology.

ISC has issued a series of physical security standards and guidance to assist member agencies with developing their risk assessment methodologies, but does not know the extent to which its 53 member agencies comply with its standards, including its risk assessment standards, because it does not monitor agencies' compliance. ISC does not monitor compliance or have an approach to do so that incorporates outreach to agencies regarding their compliance status. Officials stated that they would like to monitor agencies' compliance, but limited resources and other priorities, such as developing standards and guidance, have prevented them from doing so. However, ISC has the authority to create a working group from its member agencies to help it perform its duties. In the absence of ISC's monitoring, agencies' risk assessment methodologies may not align with ISC's standards. In addition, although ISC issued risk assessment guidance in August 2013, this guidance is limited. For example, the guidance does not describe how to incorporate threat, consequence, or vulnerability assessments of specific undesirable events into a risk assessment methodology. Not having appropriate guidance is inconsistent with federal internal-control standards designed to promote effectiveness and efficiency.

Contents

Figures

Abbreviations

DHS	Department of Homeland Security
DOD	Department of Defense
DOE	Department of Energy's Office of Health, Safety, and Security
DOI	Department of the Interior's Office of Law Enforcement and Security
DOJ	Department of Justice's Justice Protective Service
FEMA	Federal Emergency Management Agency
FPS	Federal Protective Service
FSL	facility security level
GSA	General Services Administration
ISC	Interagency Security Committee
LOP	level of protection
NIPP	*National Infrastructure Protection Plan*
NRC	Nuclear Regulatory Commission
OPM	Office of Personnel Management
RMP	*Risk Management Process for Federal Facilities*
State	Department of State's Bureau of Diplomatic Security
UK	United Kingdom
VA	Department of Veterans Affairs

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

March 5, 2014

The Honorable Jeff Duncan, Chairman
Subcommittee on Oversight and Management Efficiency
Committee on Homeland Security
House of Representatives

Dear Mr. Chairman:

The 2012 shooting at the Anderson Federal Building in Long Beach, California, and the 2013 shooting at the Washington Navy Yard in Washington, D.C., demonstrate that federal facilities and their employees, as well as the public who visit government buildings, continue to be the targets of violence. The Department of Homeland Security's (DHS) Federal Protective Service (FPS) and about 30 other federal agencies are responsible for protecting civilian federal facilities and their occupants from violent threats or acts, in part, by assessing risks to their facilities. However, our past work has raised questions about agencies' abilities to assess risks to federal facilities. Essentially, assessing risk involves evaluating *threats* (the intentions and capabilities of adversaries to initiate undesirable events), *consequences* (the level, duration, and nature of losses resulting from undesirable events), and *vulnerabilities* (weaknesses in the design or operation of a facility that adversaries can exploit), and recommending protective measures to mitigate risk. For example, we reported in 2012 that FPS was not assessing risks to over 9,000 facilities under the custody and control of the General Services Administration (GSA) in a manner that aligned with federal standards.[1]

To help federal agencies protect and assess risks to their facilities, the Interagency Security Committee (ISC)—a DHS-chaired organization comprised of 53 member agencies—developed a physical security standard, *The Risk Management Process for Federal Facilities (RMP)*,[2]

[1] GAO, *Federal Protective Service: Actions Needed to Assess Risk and Better Manage Contract Guards at Federal Facilities*, GAO-12-739 (Washington, D.C.: Aug. 10, 2012).

[2] Interagency Security Committee, *The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard* (August 2013).

with which federal executive branch agencies must comply.[3] Among other things, the *RMP* includes standards for agencies' facility risk assessment methodologies. According to ISC, risk assessment methodologies that meet its standards allow federal agencies to determine whether a facility's existing protective measures are sufficient to mitigate risk and, if not, identify the most cost-effective protective measures to reduce risks to an acceptable level. Given the challenges FPS faces assessing risks to federal facilities, you asked us to review how it and other federal agencies are assessing risks to their facilities.

This report addresses the following questions:

- To what extent do selected ISC member agencies' facility risk assessment methodologies align with ISC's risk assessment standards?
- How does ISC assist member agencies in developing risk assessment methodologies and monitor their compliance with these standards?

In addition, we describe in appendix II several risk assessment approaches used by foreign governments and private entities that could inform federal agencies' risk assessment methodologies.

To determine the extent to which selected ISC member agencies' facility risk assessment methodologies align with ISC's standards, we selected nine of the 53 ISC member agencies that are required to comply with ISC standards. We selected the nine agencies to achieve diversity with respect to the agencies' missions, number of facilities, and ISC membership type (primary or associate member agency).[4] Selected agencies are: the Department of Energy's Office of Health, Safety, and Security (DOE), the Department of the Interior's Office of Law Enforcement and Security (DOI), the Department of Justice's Justice Protective Service (DOJ), the Department of State's Bureau of Diplomatic

[3] ISC was created pursuant to Executive Order 12977, 60 Fed. Reg. 54411 (Oct. 19, 1995), which was subsequently amended by Executive Order 13286, 68 Fed. Reg. 106190 (March 5, 2003). ISC is housed within DHS's National Protection and Programs Directorate, Office of Infrastructure Protection.

[4] Executive Order 12977 designates certain federal agencies as ISC members. ISC refers to these agencies as primary members and other affiliated agencies as associate members. All members perform the same functions except primary agencies vote to approve ISC standards while associate members do not. See appendix III for a list of ISC member agencies.

Security (State), the Department of Veterans Affairs (VA), the Federal Emergency Management Agency (FEMA), the Federal Protective Service (FPS), the Nuclear Regulatory Commission (NRC),[5] and the Office of Personnel Management (OPM). We compared each selected agency's risk assessment methodology to ISC's risk assessment standards, which are outlined in the *RMP*. These standards generally require agencies to consider, at a minimum, all the undesirable events in the *RMP* and assess the threat, consequences, and vulnerability to specific undesirable events. We also interviewed officials about their agencies' risk assessment methodologies and reviewed documentation. For more information about how we determined the extent to which agencies' methodologies align with ISC's risk assessment standards, see appendix I. 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 agencies' facility risk assessment methodologies. In addition, because ISC is required to take such actions as may be necessary to enhance the quality and effectiveness of security in and protection of federal facilities government-wide, any recommendations we make will be to ISC and not individual agencies.

To determine how ISC assists member agencies in developing risk assessment methodologies and monitors their compliance with its risk assessment standards, we reviewed documentation and interviewed ISC officials about their efforts in these areas. We also interviewed officials from the nine selected ISC member agencies regarding ISC's risk assessment assistance, including its risk assessment guidance contained in the *RMP*. In addition, to assess the comprehensiveness of ISC's risk assessment guidance, we compared the *RMP's* guidance to federal risk assessment guidance contained in DHS's *National Infrastructure Protection Plan (NIPP)*. Like the *RMP*, the *NIPP* sets forth a risk management framework, as well as risk assessment standards and guidance. However, the *NIPP*'s standards and guidance are intended to apply broadly to 16 critical infrastructure sectors, including—but not limited to—government facilities. We also reviewed GAO's *Standards for Internal Control in the Federal Government*[6] because internal controls

[5] According to NRC, ISC standards apply only to NRC facilities and not to the nuclear facilities it regulates or the security of radioactive material.

[6] GAO, *Standards for Internal Control in the Federal Government*, GAO/AIMD-00-21.3.1 (Washington, D.C.: November 1999).

play a significant role in helping agencies achieve their mission- related responsibilities.

To identify approaches that could help inform agencies' risk assessment methodologies, we interviewed officials from foreign government agencies in Canada and the United Kingdom (UK) who are responsible for conducting risk assessments for government facilities. These government agencies were selected based on our review of previous risk assessment of federal facilities and management reports, as well as discussions with industry stakeholders about risk assessments. In addition, we interviewed security officials at a range of non-federal entities—such as multi-national corporations, hospitals, and universities—in four locations: Washington, D.C.; Boston, Massachusetts; Dallas/Fort Worth, Texas; and San Francisco, California. We selected these locations because of their geographic diversity and large population.[7] Within these locations, we selected non-federal entities that are potential targets for terrorism and other acts of violence because of their symbolism, historical significance, uniqueness, or prominence. See appendix I for more details on our scope and methodology.

We conducted this performance audit from June 2012 to March 2014 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 the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

The ISC was established by Executive Order 12977 following the 1995 bombing of the Alfred P. Murrah Federal Building in Oklahoma City, Oklahoma. Aside from certain intelligence-related exceptions, the Executive Order requires executive branch departments and agencies to cooperate and comply with ISC's policies and recommendations,

[7] Large metropolitan population was used as a proxy measure to identify major centers of economic and federal activity. We selected metropolitan areas with at least a million residents, according to the U.S. Census Bureau.

including any standards that it sets.[8] ISC's mandate is to develop and evaluate security standards for federal facilities, develop a strategy for ensuring compliance with these standards, and oversee the implementation of appropriate protective security measures in federal facilities, among other things.[9] ISC member agencies develop and draft ISC policies and standards through participation in sub-committees and working groups. In addition, all ISC member agencies have an opportunity to review and comment on ISC draft standards, and the 21 primary member agencies vote to approve final ISC standards.

From 2008 through 2013, ISC issued a series of standards to assist federal agencies in developing and implementing physical security programs at federal facilities, including standards for facility risk assessment methodologies. In August 2013, ISC combined six existing ISC standards—including *The Design Basis Threat, Facility Security Level Determinations for Federal Facilities*, and *Physical Security Criteria for Federal Facilities*—into a single standard, *The Risk Management Process for Federal Facilities (RMP)*. According to ISC, the *RMP* is intended to provide agencies with an integrated, single source of physical security information and guidance.

The *RMP* also outlines the risk management process federal agencies must follow to determine which protective measures—such as identification badges, blast resistant windows, and intrusion detection systems—should be in place at their facilities (see fig. 1). The protective measures included in the *RMP* are intended to mitigate federal facilities' vulnerabilities to specific undesirable events that ISC has identified as

[8] ISC's policies, recommendations, and standards do not apply to legislative branch agencies and federal facilities occupied by military employees. However, in December 2012 the Department of Defense (DOD) directed its components to adopt ISC's standards for DOD-leased facilities located outside of military installations.

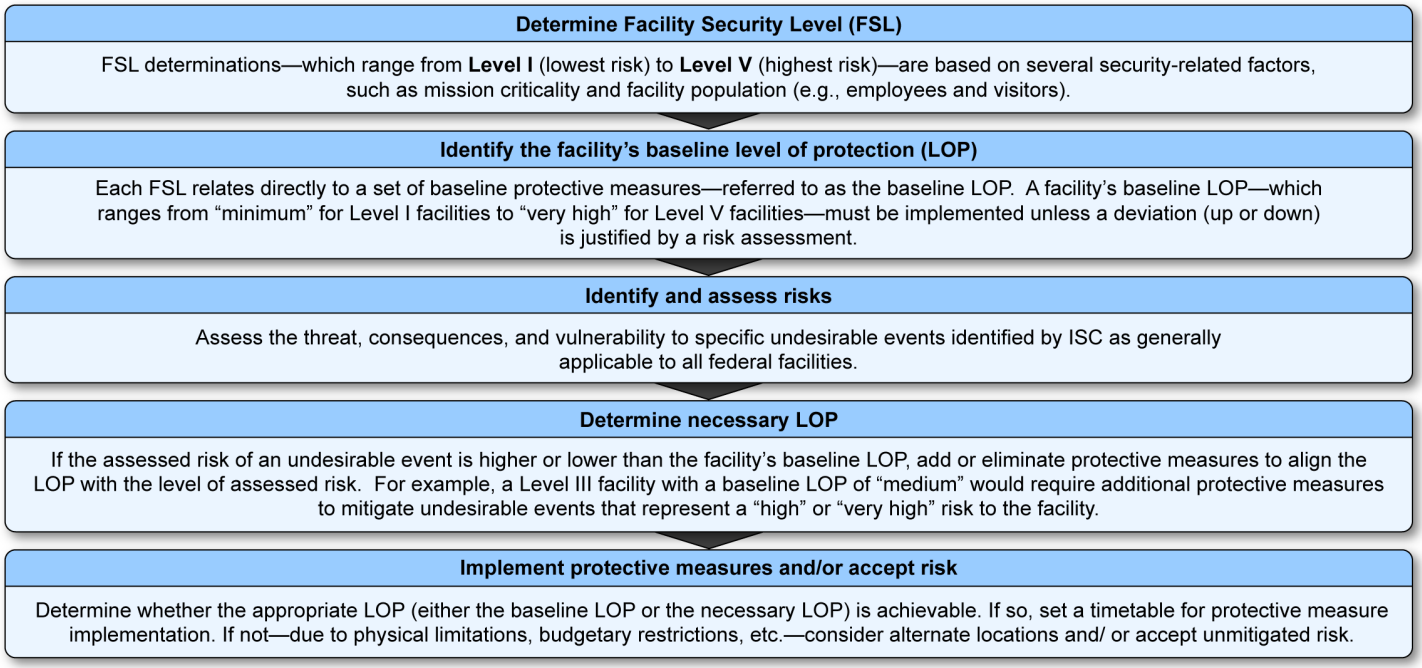
[9] This report and Executive Order 12977 refer to buildings and facilities in the United States occupied by federal employees for nonmilitary activities as "federal facilities."

generally applicable to all federal facilities.[10] To determine which undesirable events pose the greatest risk to their facilities and, therefore, which protective measures should be in place, the *RMP* requires agencies to conduct risk assessments for each of their facilities.[11] Based on the results of a risk assessment, agencies can customize (i.e., add or eliminate) the protective measures included in the *RMP* to adequately reflect the assessed level of risk.

[10] According to ISC, its undesirable events are intended to represent the "reasonable worst case scenario" for each threat. For instance, although the threat of an active shooter could manifest itself in a variety of forms—depending on the number of shooters, types of weapons used, and other tactics—ISC's *RMP* describes the active shooter event that intelligence sources suggest federal facilities should reasonably be protected against. The undesirable events identified in the *RMP* are not intended to capture the entire range of undesirable events that may affect federal facilities. As a result, the *RMP* encourages agencies to identify and assess other undesirable events that are applicable to their facilities.

[11] Risk assessments are to be conducted at least once every 5 years for lower level facilities and at least once every 3 years for higher-level facilities. For example, a lower level facility can have fewer than 100 employees and its mission criticality, symbolism, and threat are low. In contrast, a higher level facility can have over 750 employees and its mission criticality, symbolism, and threat are very high.

Figure 1: Summary of the Interagency Security Committee's Risk Management Process, as of August 2013



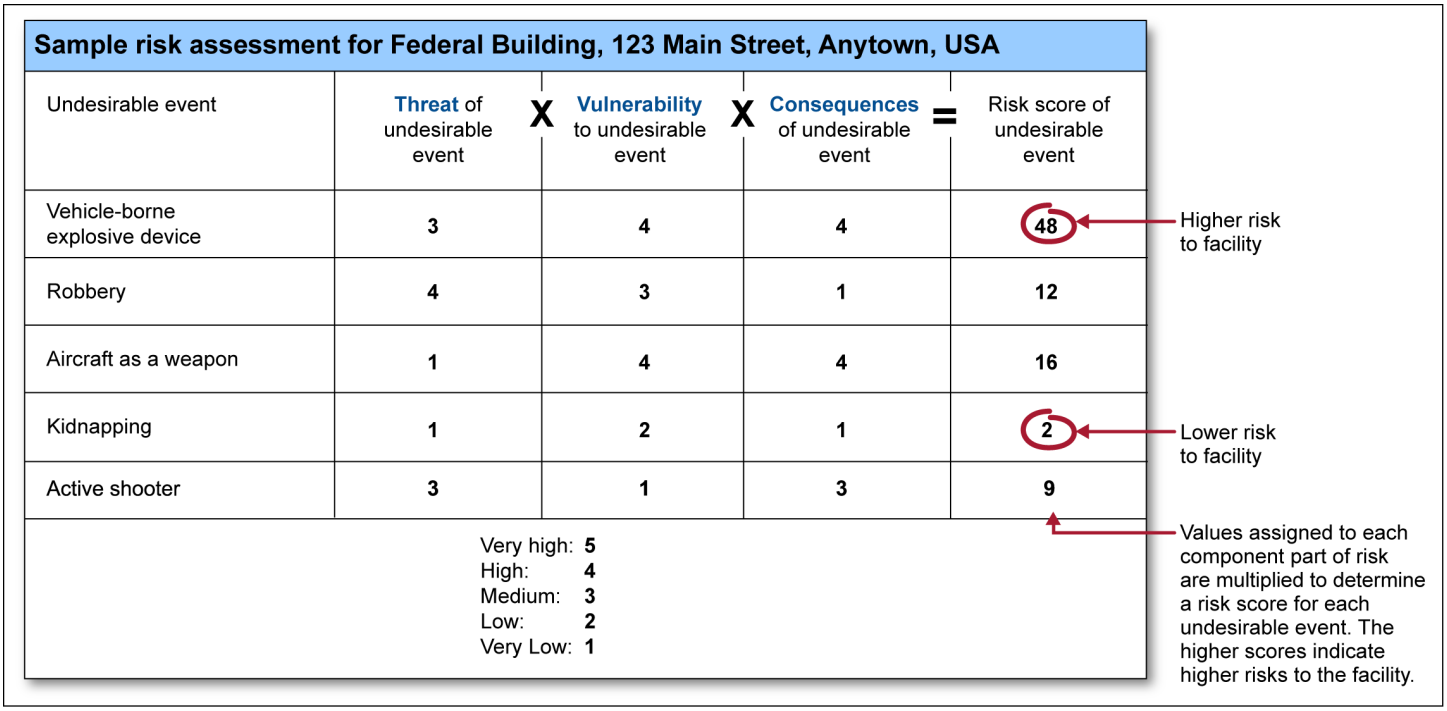
Source: GAO analysis of Interagency Security Committee information.

Because risk assessments play a key role in ISC's risk management framework, the *RMP* includes standards for agencies' facility risk assessment methodologies. Specifically, the *RMP* requires that agencies' risk assessment methodologies must: (1) consider all of the 31 undesirable events in the *RMP*, and (2) assess the threat, consequences, and vulnerability to specific undesirable events. While the sources vary, agencies might obtain threat information through intelligence analyses, vulnerability information from facility site visits, and consequence information from interviews with tenants and facility managers.

In their basic form, risk assessment methodologies involve assigning ratings to each of the three component parts of risk—threat, vulnerability, and consequence—and combining these ratings—such as through multiplication—to produce an overall estimate of risk for each identified undesirable event. In our hypothetical risk assessment example shown in figure 2, each component of risk is assigned a rating between 1 (Very Low) and 5 (Very High) based on the facility's conditions; these ratings are then multiplied to produce an overall estimate of risk for each undesirable event. This hypothetical assessment identified the "vehicle-

borne explosive device" undesirable event as the highest risk to the facility and "kidnapping" as the lowest risk. Facility managers can use this and other information resulting from a risk assessment to make security-related decisions and direct resources to address any unmitigated risk.

Figure 2: Hypothetical Example of Basic Risk Assessment Methodology Applied to a Federal Facility



Source: GAO analysis of Interagency Security Committee information.

Note: The values used in the example range between 1 and 5, but an agency could choose other values, such as a range between 1 and 100 or a color scheme, to represent the same conditions.

Most Selected ISC-Member Agencies' Risk Assessment Methodologies Do Not Fully Align with ISC's Risk Assessment Standards

Three of the nine selected agencies' risk assessment methodologies we reviewed (DOE, DOJ, and State) fully align with ISC's *RMP* standard, but six (NRC, OPM, FEMA, FPS, VA, and DOI) do not, as shown in table 1. As a result, these six agencies may not have a complete understanding of the risks facing their approximately 52,000 federal facilities and may be less able to allocate security resources cost-effectively either at the individual facility level or across their portfolio of facilities.

Table 1: Six of Nine Selected ISC Member Agencies' Risk Assessment Methodologies Do Not Fully Align with ISC's Risk Assessment Standards

ISC member agency[a]	Number of facilities[b]	Does the methodology consider all of the undesirable events in the *RMP*?[c]	Does the methodology assess the threat of specific undesirable events?	Does the methodology assess the consequences of specific undesirable events?	Does the methodology assess the vulnerability to specific undesirable events?
DOE	3	Y	Y	Y	Y
DOJ	13	Y	Y	Y	Y
State	140	Y	Y	Y	Y
NRC	12	Y	Y	N	Y
OPM	72	N	Y	Y	Y
FEMA	89	Y	Y	Y	N
FPS	9,600	Y	Y	N	N
VA	7,628	N	Y	Y	N
DOI	34,914	N	N	N	N
Total	**52,471**				

Source: GAO analysis of agency information.

[a]Several of our selected agencies have multiple agency components or divisions that conduct facility risk assessments. For example, the U.S. Marshal Service within DOJ also conducts facility risk assessments. However, we selected and interviewed the agency division that is responsible for assessing risk to the agency's headquarters facility (or facilities).

[b]This report and Executive Order 12977 refer to buildings and facilities in the United States occupied by federal employees for nonmilitary activities as "federal facilities." We asked agencies to report the number of facilities in their portfolio that meet this definition and apply to their risk assessment methodology. FPS provided an approximate number because it said its number of facilities is continually changing. DOI did not provide a number. Instead, we determined an approximate number of DOI facilities based on our analysis of Federal Real Property Profile data. See appendix I.

[c]ISC's risk assessment standards require that federal agencies' risk assessment methodologies (1) consider all of the undesirable events in the *RMP* and (2) assess the threat, consequences, and vulnerability to specific undesirable events.

Three of the Nine Selected Agencies' Risk Assessment Methodologies Fully Align with ISC's Risk Assessment Standards

ISC's risk assessment standards require that federal agencies' risk assessment methodologies (1) consider all of the undesirable events in the *RMP* and (2) assess the threat, consequences, and vulnerability to specific undesirable events. We found that DOE, DOJ, and State have a risk assessment methodology that meets these standards. DOJ's methodology, which was also adopted by State, documents that all of the undesirable events in the *RMP* were considered. It also assesses the threat, consequences, and vulnerability to each undesirable event. Specifically, each undesirable event in the *RMP*—such as vehicle-borne explosive device—is initially assigned a baseline rating for each component of risk. These baseline ratings —which range from 1 (lowest) to 5 (highest)—are based on information and analysis from the *RMP*. For example, DOJ uses the facility's facility security level (FSL) as the baseline consequence rating for each undesirable event. As a result, if a facility's FSL is determined to be a Level 3, then all of the undesirable events listed in the *RMP* are initially given a consequence rating of 3. A DOJ official explained that assessors then adjust the baseline ratings up or down as necessary to reflect the facility's actual conditions. In addition, DOJ officials informed us that the reasoning behind any adjustments to the baseline ratings must be documented as part of the assessment. The final risk scores for each undesirable event reflect the adjusted ratings, if any.

DOE's methodology also considers all undesirable events in the *RMP* and assesses the threat, consequences, and vulnerability to specific undesirable events. DOE officials explained that they combine the *RMP*'s baseline threat ratings for each undesirable event—such as aircraft as a weapon, hostile surveillance, and kidnapping—with consequence ratings to determine a "significance rating" for each undesirable event. Each event also then receives a vulnerability assessment and score, but DOE conducts more comprehensive vulnerability assessments for undesirable events with higher significance ratings. DOE subsequently multiplies all three ratings (threat, consequence, and vulnerability) to obtain an overall estimate of risk for each undesirable event.

Six of the Nine Selected Agencies' Risk Assessment Methodologies Do Not Fully Align with ISC's Risk Assessment Standards

The remaining six agencies we reviewed—NRC, OPM, FEMA, FPS, VA, and DOI—do not have a risk assessment methodology that fully aligns with ISC's standards because as shown in table 1, they contain one or more of the following limitations:

- they do not consider all of the undesirable events in the *RMP*, and
- they do not assess threat, consequences, and/or vulnerability to specific undesirable events.

Some Agencies' Methodologies Do Not Consider All *RMP's* Undesirable Events

Three agencies' methodologies we reviewed (OPM, VA, and DOI) do not consider all of the undesirable events included in the *RMP*. According to an ISC official, an agency's methodology must include, as a starting point or baseline, all of the undesirable events listed in the *RMP*; however, agencies have the flexibility to omit events they determine are not applicable to their facilities (or a particular facility) or add events that are not included in the *RMP* as long as these changes are documented. For example, although OPM's methodology includes some of the *RMP*'s undesirable events—such as arson, assault, and kidnapping—others are omitted, such as aircraft as a weapon and coordinated or sequential attack. An OPM official informed us that their methodology lacks some of the *RMP*'s undesirable events because it was developed before ISC issued its risk assessment standards in 2010. However, the official also informed us that they are modifying their methodology to include all of the undesirable events in the *RMP*.[12] VA's methodology also does not consider all the undesirable events in the *RMP*; instead, it incorporates VA's list of undesirable events: assaults, physical threats of violence, illegal weapons, suicidal behavior, thefts and vandalism, and explosive devices. Officials from VA said that they do not use all of the undesirable events in the *RMP* because they find it more practical to focus on fewer events and these six events are indicative of a facility's overall safety and security. Because these agencies do not consider all of the undesirable events in the *RMP*, they may not have a complete understanding of the risks facing their facilities.

[12] In technical comments on the draft report, OPM said it had completed the modifications to its methodology to include all of the RMP's undesirable events.

Some Agencies Do Not Assess Threat, Consequences, or Vulnerability to Specific Undesirable Events

Five agencies' methodologies we reviewed (NRC, FEMA, FPS, VA, and DOI) do not assess one or more of the three components of risk required by ISC. In other words, these agencies' methodologies do not rate or score specific undesirable events for all three components of risk (threat, consequences, and vulnerability). As shown in table 1, DOI's methodology does not align with any of ISC's risk assessment standards. DOI officials told us that the department's methodology does not align with ISC standards, in part, because of challenges presented by its broad and diverse missions and a lack of resources and expertise to conduct risk assessments.

Although the other four agencies' methodologies we reviewed (NRC, FEMA, FPS, and VA) are consistent with some aspects of ISC's risk assessment standards, they lack an assessment of one or more of the components of risk. For instance, as we have previously reported, FPS's current methodology does not assess consequences. FPS stated that it intends to eventually incorporate consequence into its risk assessment methodology and is exploring ways to do so. NRC's methodology also does not assess the consequences of specific undesirable events. According to NRC officials, the agency does not believe it is necessary to conduct a consequence analysis for each undesirable event. However, NRC's vulnerability assessment approach aligns with ISC's risk assessment standards. Specifically, for each undesirable event in the *RMP*, NRC calculates a percentage-based vulnerability score that represents the number of protective measures that are currently in place and applicable to that undesirable event. For example, if 50 protective measures are applicable to an active-shooter undesirable event and the facility has 25 of the applicable protective measures in place, it receives a vulnerability score of 50 percent for an active shooter event. In contrast, VA's methodology does not assess vulnerability to specific undesirable events. VA officials informed us that the department's vulnerability assessment approach was developed before ISC issued its risk assessment standards in 2010 and that VA is modifying its approach to better align with ISC's standards.

In contrast to these five agencies, some government agencies in Canada and the United Kingdom have a risk assessment methodology that assesses the consequences of and vulnerability to specific undesirable events, as shown in appendix II.

Because their risk assessment methodologies do not align with ISC's risk assessment standards, these six agencies we reviewed may not have a complete understanding of the risks facing approximately 52,000 federal

facilities located around the country. If, for example, an agency's methodology does not consider all the undesirable events in the *RMP*, or does not assess all three components of risk (threat, vulnerability, and consequence), then the agency would have an incomplete picture of risk at facilities assessed using this methodology. Moreover, because risk assessments play a critical role in helping agencies tailor protective measures to reflect their facilities' unique circumstances and risks, these agencies might not allocate security resources effectively—that is, they might provide too much or too little protection at their facilities or across their facility portfolios.

ISC Does Not Know If Member Agencies Are Complying with Its Standards, and Its Risk Assessment Guidance Could Be Enhanced

ISC Does Not Know Whether Member Agencies Are Complying with Its Standards

ISC has taken some steps to assist member agencies with their risk assessment methodologies. Most notably, since 2008, ISC has issued a series of physical security standards and guidance, including standards and guidance on facility risk assessment methodologies. ISC also started a program in 2012 to certify that member agencies' risk assessment tools met its standards.[13] As of November 2013, ISC had certified DOJ's tool as ISC-compliant. However, ISC does not know the extent to which its member agencies are complying with its standards, including its risk assessment standards, because it does not monitor agencies' compliance with its standards.[14]

[13] Some agencies apply their risk assessment methodologies using a tool, such as a software program or an automated spreadsheet.

[14] Because ISC is required to take such actions as may be necessary to enhance the quality and effectiveness of security in and the protection of federal facilities government-wide, any recommendations we make will be to ISC and not individual agencies.

According to a senior ISC official, ISC does not monitor agencies' compliance and has not developed an approach to do so that includes conducting outreach to determine the extent of compliance. Executive Order 12977 places responsibility for monitoring federal agency compliance with the Secretary of DHS; however, this ISC official noted that establishing a monitoring process and ensuring compliance are both goals listed in the Committee's 2012- 2017 Action Plan.

ISC officials told us that they would like to monitor agencies' compliance with ISC standards, but limited resources[15] and other priorities, such as developing standards and guidance, have prevented the ISC from doing so. Federal internal-control standards state that monitoring is an essential management control because it allows agencies to assess the effectiveness of a program and take corrective action as necessary.[16] Without monitoring agencies activities via appropriate mechanisms, ISC does not know the extent to which member agencies understand and are complying with its standards, including its risk assessment standards, and whether the standards are effective. Moreover, in the absence of ISC's monitoring, as illustrated by our examples above, agencies are interpreting or implementing the standards in different ways. As the government's central forum for sharing information and guidance on physical security, ISC also has the authority to create a working group to help it conduct outreach to determine the extent of compliance with its *RMP* standard.[17] Such outreach may result in better use of the *RMP* standard and ultimately enhanced protection of federal facilities.

ISC's Risk Assessment Guidance in the *RMP* Is Limited and Could Be Enhanced

ISC's *RMP* outlines ISC's risk assessment standards and related guidance. However, we found that this guidance is limited as compared to federal risk assessment guidance contained in DHS' *National Infrastructure Protection Plan (NIPP)*.[18] For example, the *RMP* does not describe how to incorporate threat, consequence, or vulnerability

[15] As of November 2013, ISC had a staff of 7 full time employees.

[16] GAO/AIMD-00-21.3.1.

[17] ISC has the authority to establish working groups composed of participants from member agencies to perform tasks as directed by the ISC.

[18] The *NIPP* sets forth a risk management framework and risk assessment standards that are intended to apply broadly to 16 critical infrastructure sectors, including—but not limited to—government facilities.

assessments of specific undesirable events into a risk assessment methodology. As a result, some agencies we reviewed may continue to face challenges developing methodologies that align with ISC standards. In addition, federal internal control standards state that federal agencies should have appropriate guidance for each of their activities.[19]

As compared to the *NIPP*, ISC's *RMP* lacks specificity. Although the scope and applicability of the *NIPP* is broader than the *RMP*, the *NIPP* contains more detailed information and guidance on risk assessments. For example, unlike the *RMP*, the *NIPP* contains dedicated sections on threat assessment, vulnerability assessment, and consequence assessment. In each of these sections, the *NIPP* provides "core criteria guidance" that generally covers the scope of the assessments, key factors that should be estimated, and documentation requirements, among other things. In contrast, the *RMP* does not include these items; it also does not provide examples of risk assessment methodologies that align with ISC's risk assessment standards.

In addition, officials from three agencies we reviewed told us that the risk assessment section of ISC's *RMP* lacks specificity and could be enhanced. For instance, officials from one agency said that although ISC has provided federal agencies with specific information and guidance in many areas, it does not provide detailed guidance on risk assessment methodologies. These agency officials also noted that because ISC's risk assessment guidance is limited, it might not be useful to agencies that do not have extensive physical-security resources and expertise. Similarly, officials from another agency told us that it would be helpful if ISC expanded its risk assessment guidance to include examples of acceptable risk assessment methodologies, including potential ways to evaluate and categorize threats, vulnerabilities, and consequences.

ISC officials informed us that they have not provided more detailed risk assessment guidance, examples of methodologies that align with its standards, or other resources in the *RMP* because member agencies have not requested this information. However, agencies may not be requesting additional guidance and information from ISC because they are unaware their risk assessment methodologies, or aspects of their methodologies, are inconsistent with ISC's standards. Three of the six

[19] GAO/AIMD-00-21.3.1.

agencies we reviewed with methodologies that do not align with ISC's risk assessment standards were unaware that their methodology had limitations.

Without additional guidance and other information in the *RMP*, such as examples of methodologies that align with ISC's risk assessment standards (e.g., DOJ's methodology), some agencies may continue to face challenges developing and implementing appropriate methodologies and, therefore, remain unable to assess risks at their facilities in a manner that aligns with ISC standards. In addition, given the federal government's current fiscal challenges, additional guidance may help prevent some agencies from expending limited resources on ineffective or non-compliant risk assessment methodologies.

Conclusions

ISC, currently comprised of 53 member federal agencies, was established to enhance the quality and effectiveness of physical security in federal facilities. Its standards, including its risk assessment standards, are collectively developed and approved by representatives from ISC's member agencies; as a result, these agencies had input in determining how risks to federal facilities should be assessed. However, six of the nine selected ISC member agencies we reviewed do not use a risk assessment methodology that aligns with the standards. As a result, these agencies may not have a complete understanding of risk—and may be ineffectively allocating security resources—at approximately 52,000 federal facilities and across the agencies' portfolio of facilities.

Although risk assessments play a critical role in ISC's risk management framework, ISC does not know the extent to which its member agencies' risk assessment methodologies align with its standards because it does not monitor compliance or have an approach to do so that incorporates outreach to agencies regarding their compliance status. As the government's central forum for sharing information and guidance on physical security, ISC has the authority to create a working group to help it conduct outreach to determine the extent of compliance with its *RMP* standard. Such outreach may result in better use of the standard and ultimately better protection of federal facilities. Moreover, given the federal government's current fiscal challenges, additional risk assessment guidance—that includes examples of methodologies that align with ISC's standards—could help prevent federal agencies from expending their limited resources on methodologies that are not ISC-compliant.

Recommendations for Executive Action

To help ensure that federal agencies are developing and using appropriate risk assessment methodologies, the Secretary of Homeland Security should direct the ISC to take the following two actions:

- conduct outreach to identify which member agencies have not developed risk assessment methodologies that align with ISC standards and develop a mechanism to monitor and ensure compliance of all its member agencies, and
- supplement the risk assessment guidance contained in *The Risk Management Process for Federal Facilities* with: (1) information on how to incorporate threat, consequence, and vulnerability assessments of specific undesirable events into a risk assessment methodology and (2) examples of risk assessment methodologies that ISC determines comply with its standards.

Agency Comments

We sent a draft of this report to the Department of Homeland Security (including the Federal Protective Service and Federal Emergency Management Agency), Interagency Security Committee, Department of Energy, Department of the Interior, Department of Justice, Department of State, Department of Veterans Affairs, Nuclear Regulatory Commission, and Office of Personnel Management for review and comment. DHS provided written comments and concurred with our recommendations; see appendix IV.

NRC, OPM, FEMA, FPS, DOI, and ISC also provided technical comments, which we incorporated as appropriate. In technical comments, DOI disagreed with our assessment of whether its risk assessment methodology aligns with ISC's *RMP* but did not provide any additional documentation for our consideration. We continue to believe that our assessment of DOI's methodology is accurate based on our understanding and application of ISC's *RMP*. DOE, DOJ, State, and VA did not have any comments on the draft report.

As agreed with your office, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the report date. At that time, we will send copies of this report to the Secretary of Homeland Security, appropriate congressional committees, and other interested parties. In addition, the report will be available at no charge on the GAO Web site at http://www.gao.gov.

If you or your staff have any questions on this report, please contact me at (202) 512-2834 or GoldsteinM@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Contact information and key contributors to the report are listed in appendix V.

Sincerely yours,

Mark Goldstein
Director, Physical Infrastructure Issues

Appendix I: Objectives, Scope, and Methodology

Our report addresses the following questions: 1) To what extent do selected ISC member agencies' facility risk assessment methodologies align with ISC's risk assessment standards? 2) How does ISC assist member agencies in developing risk assessment methodologies and monitor their compliance with these standards? In addition, we describe several risk assessment approaches used by non-federal entities and foreign governments that may inform federal agencies' risk assessment methodologies.

To determine the extent to which selected ISC-member agencies' facility risk assessment methodologies align with ISC standards, we selected a non-generalizable sample of nine ISC member agencies (out of 53) and interviewed officials and obtained documentation about their risk assessment methodologies. We limited the scope of our review to federal agencies that are ISC members and required to comply with ISC standards to ensure that each federal agency in our review is familiar with and potentially adhering to ISC's risk assessment standards (see app. III for a list of ISC member agencies).[1] The nine agencies were chosen to achieve diversity with respect to their missions, ISC membership type, and size. More specifically, we sought to achieve a mix of law-enforcement and non-law-enforcement agencies, primary and associate ISC member agencies, and large, medium, and small agencies.[2] The nine agencies selected include: Department of Energy, Office of Health, Safety, and Security; Department of Interior, Office of Law Enforcement and Security; Department of Justice, Justice Protective Service; Department of State, Bureau of Diplomatic Security; Department of Veterans Affairs; Federal Emergency Management Agency; Federal

[1] Aside from certain intelligence-related exceptions, each executive agency and department is to cooperate and comply with the policies and recommendations of the ISC. ISC standards do not apply to legislative branch agencies and federal facilities occupied by federal military employees.

[2] For the purposes of this report, an agency was categorized as large if it had more than 1,000 facilities; medium if it had between 50 and 1,000 facilities; and small if it had less than 50 facilities. Information on the number of facilities was obtained through interviews with agency officials and self-reported data provided to GAO for previous facility security work (see GAO-13-222, appendix I for more information about this data).

Protective Service; Nuclear Regulatory Commission; and Office of Personnel Management.[3]

For the number of facilities listed in table 1, we asked agencies to report the number of facilities in their portfolio that meet ISC's definition of "federal facility" and apply to their risk assessment methodology.[4] Seven agencies provided us with specific numbers. FPS provided an approximate number because it said its number of facilities is continually changing. DOI did not provide a number. Instead, we determined an approximate number of DOI facilities based on our analysis of data from the Federal Real Property Profile, a centralized real property database maintained by GSA that contains data on the federal government's real property inventory. We identified the number of buildings DOI reported and then excluded categories of buildings that we thought likely did not meet ISC's definition. We provided the number to DOI for review.

In addition, we reviewed and analyzed ISC's risk assessment standards, which are outlined in ISC's *Risk Management Process for Federal Facilities (RMP)* standard. According to ISC's *RMP*, agencies' risk assessment methodologies must:

- consider all the undesirable events identified in the *RMP* as possible risks to federal facilities;[5]
- 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.

[3] Several of our selected agencies have multiple agency components or divisions that conduct facility risk assessments. For example, the U.S. Marshals Service within DOJ also conducts facility risk assessments. However, we selected and interviewed the agency divisions that are responsible for assessing risk to the agency's headquarters facility (or facilities).

[4] ISC refers to buildings and facilities in the United States occupied by federal employees for nonmilitary activities as "federal facilities".

[5] According 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 *RMP*; 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 *RMP* as long as these changes are documented.

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. Therefore, for the purposes of this report, risk assessment methodologies that align with ISC standards are those that consider all the undesirable events identified in the *RMP*, and assess the threat, consequences, and vulnerability to specific undesirable events.

To determine whether agencies' methodologies align with the above stated criteria, we reviewed and analyzed information regarding each agency's risk assessment methodology to answer the following four questions:

1. Does the methodology consider all of the undesirable events in the *RMP*?[6]
2. Does the methodology assess the threat of specific undesirable events?
3. Does the methodology assess the consequences of specific undesirable events?
4. Does the methodology 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 question 2, 3, and 4 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 four questions was "Yes," then the agency's overall risk assessment methodology aligns with ISC's risk assessment standards for the purposes of this report. If the answer to one or more of the four questions was "No", then the agency's methodology does not to align with ISC's standards for the purposes of this report.

[6] Per ISC, our determinations reflect that agencies can deem undesirable events on this list not applicable after an initial consideration and include additional undesirable events not on ISC's list as long as these changes are documented.

To determine how ISC assists member agencies in developing risk assessment methodologies and monitors their compliance, we reviewed documentation and interviewed ISC officials about their efforts in these areas. We also interviewed officials from the nine selected ISC member agencies regarding ISC's risk assessment assistance, including its risk assessment guidance contained in the *RMP*. In addition, to assess the comprehensiveness of ISC's risk assessment guidance, we compared the *RMP's* guidance to federal risk assessment guidance contained in DHS's *National Infrastructure Protection Plan (NIPP)*. Like the *RMP*, the *NIPP* sets forth a risk management framework, as well as risk assessment standards and guidance. However, the *NIPP's* standards and guidance are intended to apply broadly to 16 critical infrastructure sectors, including—but not limited to—government facilities. We also reviewed GAO's *Standards for Internal Control in the Federal Government*[7] because internal controls play a significant role in helping agencies achieve their mission related responsibilities.

To identify risk assessment approaches that could inform agencies' risk assessment methodologies, we interviewed non-federal entities in four locations: Washington, D.C.; Boston, Massachusetts; Dallas/Fort Worth, Texas; and San Francisco, California. We selected these locations because of their geographic diversity and large population.[8] In each location, we interviewed officials from a range of non-federal entities that are potential targets for terrorism because of their symbolism, historical significance, uniqueness, and/ or prominence. For example, we interviewed officials from commercial property-management firms, hospitals, universities, and state and local governments. In addition, we interviewed officials who are responsible for conducting facility risk assessments for several foreign government agencies in Canada and the United Kingdom. These countries were selected based on our review of previous risk assessment and management reports and discussions with industry stakeholders about leading risk assessment practices.[9] Because we selected these non-federal entities and foreign government agencies

[7] GAO/AIMD-00-21.3.1.

[8] Large metropolitan population size was used as a proxy measure to identify major centers of economic and federal activity. We selected metropolitan areas with at least a million residents, according to the U.S. Census Bureau.

[9] We were unable to obtain information from two additional countries that met our selection criteria.

as part of a non-probability sample, our findings regarding the examples of risk assessment approaches are not generalizable.

Moreover, because ISC is responsible for developing physical security standards and ensuring compliance with them and the selected agencies we reviewed are ISC's members, any recommendations we make will be to ISC instead of individual federal agencies.

We conducted this performance audit from June 2012 to March 2014 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 the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: Examples of Other Organizations' Approaches to Assessing Vulnerability and Consequence

We identified how foreign governments in Canada, the United Kingdom (UK), and non-federal entities, such as hospitals, are assessing risk at their facilities, specifically their approaches for assessing the consequences of and vulnerability to undesirable events.

- Royal Canadian Mounted Police's Risk Assessment Approach: Risk assessment guidance published by a Canadian government agency includes a basic vulnerability assessment approach. Each undesirable event is rated qualitatively (High, Medium or Low) on two factors:
  1. How the vulnerability affects the severity of the undesirable event.
  2. How the vulnerability affects the likelihood that a facility will be compromised.

  A matrix that reflects both factors is used to determine the final vulnerability rating for each undesirable event. For example, a vulnerability that has a "High" impact on the severity of the undesirable event and "Medium" impact on the likelihood of compromise has an overall vulnerability rating of "High," according to the vulnerability assessment matrix.

- UK Cabinet Office's Risk Assessment Approach for Local First Responders: The UK Cabinet Office provides "impact scoring scales" to assist local responders in determining the consequences of the undesirable events applicable to their areas of jurisdiction. As explained in the agency's guidance, each undesirable event should be assigned an impact score between 1 (insignificant) and 5 (catastrophic), depending on its anticipated consequences in the following areas:
  - health: includes direct impacts (numbers of people affected, fatalities, injuries, etc.) and indirect impacts that may arise due to strains on health services;
  - social impacts: includes availability of government programs and services, damage to property, disruption of communications and supply chains (e.g., money, food, water, energy, or fuel); and public disorder due to anger, fear, and/or lack of trust in the authorities;
  - economic impacts: encompasses the net economic cost, including both direct (e.g., loss of goods, buildings, infrastructure) and indirect (e.g., loss of business, increased demand for public services) costs; and
  - environmental impacts: encompasses contamination or pollution of land, water, or air, with harmful biological/chemical/radioactive

matter or oil, flooding, or disruption or destruction of plant or animal life.

Another UK government agency rates 14 undesirable events on a scale of 1 (limited) to 5 (catastrophic) based on the estimated number of casualties, reputational damage, and disruption to the business of the agency.

- U.S. Hospitals' Risk Assessment Approach: Two major hospitals we spoke with use a risk assessment methodology developed by a non-profit healthcare organization that includes an event-based consequence assessment approach. Each undesirable event is assigned a separate rating—from 0 (Not Applicable) to 3 (High)—for probability and six consequence factors: human impact, property impact, business impact, preparedness, internal response, and external response. Overall consequence ratings for each undesirable event are obtained by summing the 6 ratings and dividing the total by 30 (the highest possible sum of the 6 ratings).

Appendix III: Interagency Security Committee Primary and Associate Member Agencies

ISC Primary Members

1. Assistant to the President for National Security Affairs
2. Central Intelligence Agency
3. Department of Agriculture
4. Department of Commerce
5. Department of Defense
6. Department of Education
7. Department of Energy
8. Department of Health and Human Services
9. Department of Homeland Security
10. Department of Housing and Urban Development
11. Department of the Interior
12. Department of Justice
13. Department of Labor
14. Department of State
15. Department of Transportation
16. Department of the Treasury
17. Department of Veterans Affairs
18. Environmental Protection Agency
19. General Services Administration
20. Office of Management and Budget
21. U.S. Marshals Service

ISC Associate Members

1. Commodity Futures Trading Commission
2. Court Services and Offender Supervision Agency
3. Federal Aviation Administration
4. Federal Bureau of Investigation
5. Federal Communications Commission
6. Federal Deposit Insurance Corporation
7. Federal Emergency Management Agency
8. Federal Protective Service
9. Federal Reserve Board
10. Federal Trade Commission
11. Government Accountability Office
12. Internal Revenue Service
13. National Aeronautics & Space Administration
14. National Archives & Records Administration
15. National Capital Planning Commission
16. National Institute of Building Sciences
17. National Institute of Standards & Technology

18. National Labor Relations Board
19. Nuclear Regulatory Commission
20. National Science Foundation
21. Office of the Director of National Intelligence
22. Office of Personnel Management
23. Office of the U.S. Trade Representative
24. Securities and Exchange Commission
25. Smithsonian Institution
26. Social Security Administration
27. U.S. Army Corps of Engineers
28. U.S. Capitol Police
29. U.S. Coast Guard
30. U.S. Courts
31. U.S. Institute of Peace
32. U.S. Postal Service

Appendix IV: Comments from the Department of Homeland Security

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

Homeland Security

February 19, 2014

Mark Goldstein
Director, Physical Infrastructure Issues
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Re: Draft Report GAO-14-86, "FEDERAL FACILITY SECURITY: Additional Actions Needed to Help Agencies with Risk Assessment Methodology Standards"

Dear Mr. Goldstein:

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's) work in planning and conducting its review and issuing this report.

The Department is pleased to note that GAO recognized the efforts of the Interagency Security Committee (ISC) to improve physical security guidance to assist federal agencies with developing risk assessment methodologies to protect and assess risk to federal facilities. For example, the ISC has made efforts to assist agencies with the ISC standards in other ways. Specifically the ISC issued a series of standards and guidance, most notably the ISC's *Risk Management Process* document, to assist member agencies with developing their risk assessment methodologies, as well as to provide agencies with both classroom and online training.

The draft report contained two recommendations with which DHS concurs. Specifically, GAO recommended that the Secretary of Homeland Security direct the ISC to:

Recommendation 1: Conduct outreach to identify which member agencies have not developed risk assessment methodologies that align with its standards and develop a mechanism to monitor and ensure compliance of all its member agencies.

Response: Concur. In a 2013 report,[1] GAO noted that survey responses from 32 agencies indicated that the ISC standards are a frequently used source in developing and updating federal agency physical security programs. This was second only to institutional knowledge or subject matter expertise in physical security that agencies' security staffs have developed through their professional experience.

[1] *FACILITY SECURITY: Greater Outreach by DHS on Standards and Management Practices Could Benefit Federal Agencies*, GAO-13-222 (Washington, D.C., 1 February 2013).

This is important because, in terms of a formal outreach strategy, the ISC is in the preliminary stages of developing and assessing its outreach efforts as noted above. Through the ISC outreach program, these efforts will increase awareness and use of ISC standards and documents across the federal portfolio.

The *Interagency Security Committee Outreach Strategic Plan* provides a foundation for the ISC's implementation of outreach activities to increase awareness, understanding, and use of the ISC standards, guidelines, best practices, and white papers among federal agencies. Consistent with GAO's recommendations, the ISC developed a plan that defines the goals and objectives of future outreach efforts, specifies the target audience for outreach activities, and describes outreach options.

The ISC agrees that conducting outreach and compliance is a key part of assisting agencies with the use of the ISC's standards. It is important to note that ISC has developed a strategy for compliance that should be finalized within the next 3 months. Further, the ISC has approved a new Compliance Working Group to begin sometime in spring 2014.

The ISC is currently in the final stages of developing a strategy for compliance. The strategy should be completed by the 4th Quarter of Fiscal Year (FY) 2014. The ISC has also approved the creation of a working group chartered to use the ISC's existing authority under Executive Order 12977 to develop a strategy for ensuring compliance with established standards and to oversee the implementation of appropriate security measures in federal facilities. Estimated Completion Date (ECD): March 30, 2015.

Recommendation 2: Supplement the risk assessment guidance contained in *The Risk Management Process for Federal Facilities* with information on how to incorporate threat, consequence, and vulnerability assessments of specific undesirable events into a risk assessment methodology and examples of risk assessment methodologies that ISC determines comply with its standards.

Response: Concur. Since the release of the ISC's *The Risk Management Process for Federal Facilities*, there have been a number of working groups developed to review and enhance the current elements of the ISC's risk management process and the ISC will continue efforts to enhance risk assessment guidance. Draft guidance will be completed by the 2nd Quarter of FY 2015. In March 2012, the ISC created a Standard Operating Procedure for Risk Assessment Data Tool Validation and has reviewed a number of ISC member risk assessment tools that can be provided as examples of risk assessment tools to supplement the risk assessment process. ECD: March 30, 2015.

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,

Jim H. Crumpacker
Director
Departmental GAO-OIG Liaison Office

3

Appendix V: GAO Contact and Staff Acknowledgments

GAO Contact

Mark Goldstein, (202) 512-2834 or GoldsteinM@gao.gov

Staff Acknowledgments

In addition to the individual named above, Tammy Conquest, Assistant Director; Colin Fallon; Geoff Hamilton; SaraAnn Moessbauer; Jaclyn Nidoh; and Travis Thomson made key contributions to this report.