United States Government Accountability Office

GAO

Report to Congressional Requesters

September 2012

FEDERAL REAL PROPERTY SECURITY

Interagency Security Committee Should Implement A Lessons-Learned Process

GAO-12-901

September 2012

FEDERAL REAL PROPERTY SECURITY

Interagency Security Committee Should Implement a Lessons-Learned Process

GAO Accountability * Integrity * Reliability

Highlights

Highlights of GAO-12-901, a report to Congressional Requesters

Why GAO Did This Study

Attacks on federal facilities in the U.S. have highlighted the need to identify lessons learned from prior security incidents and apply that knowledge to security procedures governmentwide. Dozens of federal law enforcement agencies provide physical security services for domestic nonmilitary federal facilities. The ISC is responsible for developing governmentwide physical security standards and coordinating agencies to improve the protection of federal facilities. As requested, this report examines (1) the practices used to identify and apply lessons learned and how agencies have used these practices, (2) actions ISC has taken to identify and apply lessons learned from attacks on federal facilities, and (3) challenges to developing a governmentwide lessons-learned process and the strategies agencies have used to mitigate those challenges. GAO reviewed documents and interviewed officials from 35 security and law enforcement agencies with experience protecting selected tourist sites in cities in Greece, Israel, Italy, and the United States. GAO also interviewed officials from ISC and agencies known to apply lessons-learned practices.

What GAO Recommends

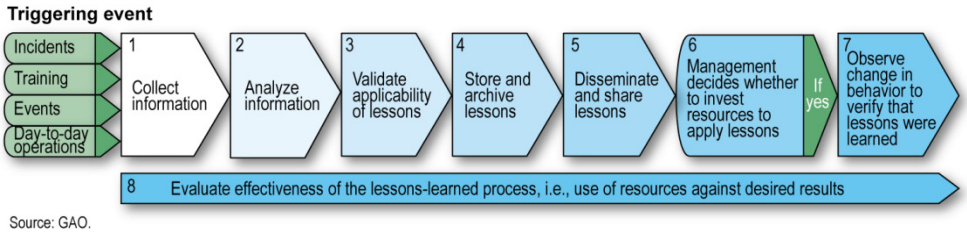
ISC should (1) incorporate the practices of a lessons-learned process as it develops its own process and (2) determine if its existing authority is sufficient to effectively implement a governmentwide lessons-learned process. DHS agreed with our findings and recommendations.

View GAO-12-901. For more information, contact Mark L. Goldstein at (202) 512-2834 or GoldsteinM@gao.gov.

What GAO Found

Based on GAO's previous work and the information obtained from other agencies, GAO identified eight individual practices that can be combined and considered steps within an overall lessons-learned process—that is, a systematic means for agencies to learn from an event and make decisions about when and how to use that knowledge to change behavior (see figure). Not all of the agencies with which GAO spoke used all of the practices, and the application of the practices varied among agencies. For example, to collect information about an incident—the first step of the process—the Bureau of Diplomatic Security within the Department of State collects incident reports, footage from security cameras, and interviews witnesses. To disseminate lessons learned—the fifth step—the Los Angeles Police Department produces a formal document after a critical incident that captures the lessons learned and disseminates the document to its units for use in planning, preparation, and coordination exercises.

A Lessons-Learned Process



Source: GAO.

The Interagency Security Committee (ISC), which is led by the Department of Homeland Security (DHS), currently does not have a systematic, comprehensive lessons-learned process for physical security, but the ISC does have a number of current initiatives that could support a more comprehensive lessons-learned effort. For example, ISC collects and analyzes information to update its physical security standards, captures and disseminates best practices to its members through its quarterly meetings, and archives information in the Homeland Security Information Network. ISC has initiated a working group to explore the idea of creating a systematic, governmentwide lessons-learned process. But the working group is at an early stage, and it is not clear if the new effort will include all of the lessons-learned practices that GAO identified. Not incorporating all eight practices could result in a less effective effort and fail to maximize the value of the lessons learned to ISC's membership. ISC derives its authority from an executive order. However, it depends on its member agencies to take the initiative to share information and it is unclear that ISC's current authority over its members is sufficient to implement a governmentwide lessons-learned process, which will rely on members to openly share information—including mistakes.

Law enforcement officials cited various challenges to establishing a governmentwide lessons-learned process, including the need to create a culture that encourages information sharing, address the concerns about safeguarding sensitive security information, disseminate information in a timely manner, and overcome resource constraints. Agencies GAO met with had found ways to mitigate these challenges using strategies consistent with a lessons-learned process.

Contents

Abbreviations

DHS	Department of Homeland Security
GAO	Government Accountability Office
GSA	General Services Administration
HSIN	Homeland Security Information Network
ISC	Interagency Security Committee
NTSB	National Transportation Safety Board
OSPB	Overseas Security Policy Board
TSWG	Technical Support Working Group

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

September 10, 2012

The Honorable Bennie G. Thompson
Ranking Member
Committee on Homeland Security
House of Representatives

The Honorable Stephen Lynch
Ranking Member
The Honorable Jason Chaffetz
Subcommittee on Federal Workforce, U.S. Postal Service and Labor Policy
Committee on Oversight and Government Reform
House of Representatives

Recent fatal attacks on federal property in the United States—such as on the U.S. Holocaust Memorial Museum in June 2009; the Lloyd D. George U.S. Courthouse in Las Vegas, Nevada, in January 2010; and Mount Rainier National Park in Washington state in January 2012—have raised concerns about how the government is identifying the lessons learned from attacks on its buildings and public spaces and using those lessons to improve security.[1] Dozens of federal law enforcement agencies secure and protect nonmilitary facilities in the United States, but the Interagency Security Committee (ISC)—an interagency organization led by the Department of Homeland Security (DHS)—develops governmentwide physical security standards and coordinates efforts to improve the protection of federal facilities. ISC was established in 1995 by Executive Order 12977 (Executive Order) following the 1995 bombing of the Alfred P. Murrah Federal Building in Oklahoma City, Oklahoma. ISC's mission is to enhance the quality and effectiveness of the security and protection of nonmilitary federal facilities in the United States and to provide a permanent body to address continuing governmentwide security issues for these facilities.

[1]According to our prior work and the work of the U.S. Army's Center for Army Lessons Learned, a lesson is knowledge or understanding gained by experience. The experience may be positive, such as a successful test or exercise, or negative, such as a mishap or failure. A lesson is learned when an organization can measure a change in behavior.

Given the importance of securing federal facilities to protect employees and the visiting public, you asked us to examine current efforts to identify lessons learned from prior security incidents and apply that knowledge to security procedures governmentwide. Our review examined:

1. if practices used to identify and apply lessons learned are applicable to the physical security of nonmilitary federal facilities and how, if at all, selected agencies have used such practices;
2. the actions that ISC has taken to identify and apply lessons learned from attacks on federal facilities since 2002; and
3. what challenges law enforcement agencies cite to developing a systematic, governmentwide process for identifying and applying lessons learned for real property security and what strategies agencies have used to mitigate those challenges internally.

To address these objectives, we reviewed documents and interviewed officials from 35 federal, local, and international agencies, including ISC. We selected the agencies based on advice from law enforcement officials and on the types of attacks experienced by the agencies. The 35 agencies included 29 law enforcement, security, or safety-related agencies (9 federal, 8 local, and 12 foreign); 4 federal agencies with responsibilities for developing physical security standards and guidelines; and 2 federal agencies that were specifically established to develop and employ lessons-learned practices. We conducted site visits in Washington, D.C.; New York, New York; Rome, Italy; Vatican City; Athens and Thessaloniki, Greece; and Jerusalem, Israel. At these site visits, we toured facilities and met with various security and law enforcement officials. In addition, we interviewed security and law enforcement officials by telephone in Las Vegas, Nevada; Los Angeles, California; and St. Louis, Missouri. For our site visits and telephone interviews, we selected locations known for drawing large groups of tourists, whether to government facilities and public spaces or to private attractions. The information obtained during the site visits and telephone interviews is not generalizable and cannot be used to represent the opinions of all law enforcement and security officials. We use the information from these site visits and interviews to provide illustrative examples throughout our report. We also met with officials from organizations experienced in applying lessons-learned practices, including officials at the National Transportation Safety Board (NTSB), the U.S. Army's Center for Army Lessons Learned, and the Department of State's Bureau of Diplomatic Security. We also reviewed previous GAO

work and other literature on the issue of identifying and applying lessons learned to improve future performance.

We conducted this performance audit from April 2011 to September 2012 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. Further details of our scope and methodology can be found in appendix I.

Background

ISC was established by Executive Order 12977 in 1995 after the Oklahoma City bombing. [2] ISC is a membership organization that currently includes 51 federal departments and agencies. The 21 initial members of ISC were identified in the executive order and 30 additional members later requested and were approved membership. ISC is housed within DHS's Office of Infrastructure Protection and has a staff of six full-time employees. The office's budget is not a dedicated line item in DHS's budget but, rather, is subsumed within the budget of the Office of Infrastructure Protection. ISC conducts much of its business through subcommittees and working groups populated by volunteers from the various member agencies. Importantly, ISC has released a body of standards that govern the physical security efforts of all federal, non-military agencies located in the U.S.—about 350,000 facilities as of fiscal year 2010.[3]

Executive Order 12977 states that ISC, among other things, shall:

- establish security and protection policies;

[2]Executive Order 12977; 60 Fed. Reg. 54411, October 24, 1995, Interagency Security Committee, as amended by Executive Order 13286; 68 Fed. Reg. 10619, March 5, 2003, which, among other things, transferred the responsibility of chairing the committee from the Administrator of the General Services Administration to the Secretary of Homeland Security.

[3]Physical 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).

- develop and evaluate security standards, develop a strategy for ensuring compliance with these standards, and oversee the implementation of appropriate security measures;
- encourage member agencies to share security-related intelligence in a timely and cooperative manner; and
- take such actions as necessary to carry out its mission.

The Executive Order requires that each executive agency cooperate with ISC and comply with its policies, standards, and recommendations and, to the extent permitted by law and subject to the availability of appropriations, provide necessary support to enable ISC to perform its duties and responsibilities. The order also states the Secretary of Homeland Security shall be responsible for monitoring federal agency compliance.

Individual Practices Used to Identify and Apply Lessons Learned Can Frame an Overall Lessons-Learned Process Applicable to Federal Facility Security

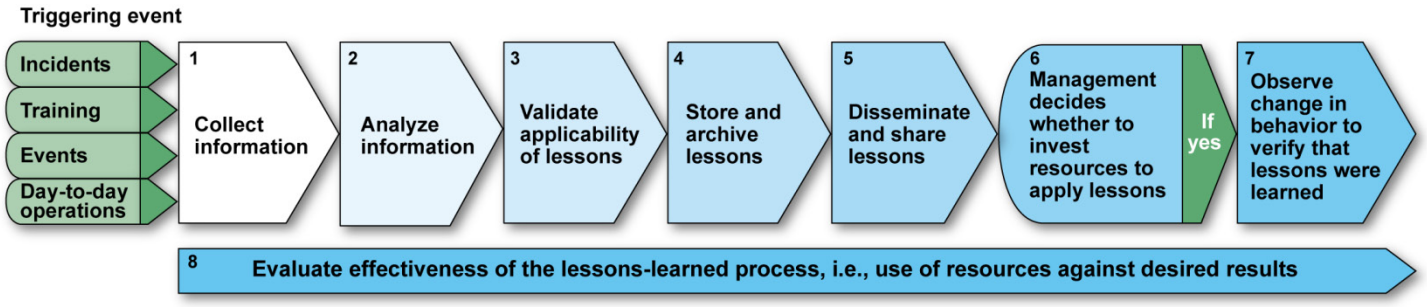
We identified eight individual practices that can be used to identify and apply lessons learned. These practices can be combined and considered steps in an overall lessons-learned process. This process could be applied to the physical security of federal buildings and public spaces. The agencies with whom we spoke provided a number of examples of how they currently use the eight practices.

Developing a Lessons-Learned Process

We identified two descriptions of a lessons-learned process: one from our prior work and one from the Center for Army Lessons Learned. We took the information from these two process descriptions, combined it with information from our reviews of lessons-learned literature and early interviews with agencies, and identified eight individual practices for identifying and applying lessons learned. We combined and ordered these practices to develop an overall, eight-step, lessons-learned process—that is, a systematic means for agencies to learn from an event and make decisions about when and how to use that knowledge to change behavior. Our lessons-learned process is shown in figure 1. We then discussed with the agencies we interviewed which practices they used in their lessons-learned efforts and how they used them. Not all

agencies used all practices, and the application of the practices varied among agencies.

Figure 1: A Lessons-Learned Process



Source: GAO.

Applying a Lessons-Learned Process to Physical Security

As shown in figure 1, the lessons-learned process consists of the eight practices, applied in a systematic order. Of the 29 federal, local, and international law enforcement, security, and safety-related agencies we reviewed, we found that only one—the State Department's Bureau of Diplomatic Security—had in place a formal physical security lessons-learned effort , called "Knowledge from the Field." Knowledge from the Field analyzes information from attacks on U.S. consulates, embassies, and personnel around the world, and then produces and distributes videos explaining the lessons learned from those attacks to the regional security officers of all the U.S. embassies and consulates. The other agencies did not have such formal lessons-learned efforts, but did conduct some of the practices related to the lesson-learned process. We thus found numerous examples of how the lessons-learned practices are currently being applied by law enforcement and security agencies—which we discuss below—that support the conclusion that the lessons-learned process as a whole is applicable to the issue of the physical security of nonmilitary federal facilities.

Collect Information

The practice of information collection involves capturing data through such activities as accident or incident reporting, project critiques, written forms, interviews of witnesses and participants, and direct observation. Information collected can be related to positive experiences that prevented accidents or saved money, or to negative experiences that resulted in undesirable outcomes. Examples of agencies collecting information as a step toward deriving lessons from incidents include the following:

- In the Knowledge from the Field initiative, the Bureau of Diplomatic Security collects incident reports submitted by regional security officers and footage from security cameras, and also interviews witnesses directly.

- Within a week of a 2010 fatal shooting at a factory, the St. Louis Metropolitan Police Department convened a meeting of the personnel involved in responding to the shooting to collect information from various perspectives about how the response had been handled.

Analyze Information

The next step in the process is to analyze the information collected to determine root causes and identify appropriate actions. Examples of agencies using information analysis as a step toward deriving lessons from incidents include the following:

- Las Vegas Metropolitan Police Department officials said that they will analyze the motives of attackers and the resulting after-action reports from a tactical operations point of view. Based on these analyses, they will adjust training and protocols.

- The Israeli National Police analyzed surveillance tape of a 2007 incident in Jerusalem involving a criminal attack on a police officer. They concluded that the officer did not show good awareness of his surroundings and that his partner was not in position to provide backup. As a result of this analysis, Israeli officials said that training was used to reinforce how officers should maintain their positions and awareness of their environments.

- Law enforcement officials in Rome conducted an after-action analysis of a 2010 riot that suggested the overwhelming presence of riot police in full protective gear may have appeared aggressive and provoked the demonstrators into violence. Since the riot, the Rome law enforcement officials have staged riot police away from the public buildings and spaces where the protests are held and the protest we observed remained peaceful.

- Although not a security agency, NTSB investigators analyze such information as aircraft wreckage, crew performance, weather data, and other pertinent information to determine the probable cause of an accident and needed corrective actions.

Validate Applicability of Lessons

Once the analysis has identified the lessons, the next practice that some agencies engaged in was to validate that the right lessons had been identified and to determine the breadth of their applicability. Subject matter experts or other stakeholders may be involved in this step of the

process. Examples of agencies using validation as a step for deriving lessons from incidents include the following:

- The U.S. Marshals convened a group of officials from related law enforcement agencies to study and validate the lessons from the January 2010 fatal shooting at the Lloyd D. George U.S. Courthouse in Las Vegas, Nevada, and to determine the extent to which the lessons might apply more broadly to physical security in the U.S. courts and other agencies.

- NTSB uses the "party system" of designating other involved organizations or companies as participants in its investigations to ensure that all of the necessary subject experts are involved to help validate the extent that the investigation's findings apply to a broader population. For example, an aircraft manufacturer can, as a party to the investigation, validate the extent to which a design flaw may apply beyond a specific aircraft under investigation.

Archive Lessons

The storage of lessons usually involves entering lessons into an electronic database to disseminate and share information. As appropriate, repositories should have the capability to store data and to guard classified, sensitive, or proprietary data. The Center for Army Lessons Learned handbook indicates that the archival process should remain an ongoing process or risk becoming cumbersome and irrelevant.[4] Examples of agencies storing and archiving lessons learned include the following:

- Federal and local law enforcement agencies we interviewed stated that they use a variety of online databases and networks for storing and sharing their experiences, including DHS's Homeland Security Information Network (HSIN) and Technical Resource for Incident Prevention ("TRIPwire"), FBI's Law Enforcement Online, FEMA's Lessons Learned Information System, and the Department of Justice's Nationwide Suspicious Activity Reporting Initiative.

[4]For example, in our previous work, we found an agency had worked to archive lessons learned, but was unable to do so in a way that program staff effectively benefited. The project managers rarely and inconsistently updated and used the lessons-learned database, according to the agency's inspector general. See GAO, *NASA: Better Mechanisms Needed for Sharing Lessons Learned*, GAO-02-195 (Washington, D.C.: Jan. 30, 2002) and NASA Office of Inspector General, *Review of NASA's Lessons Learned Information System*, IG-12-012 (Washington, D.C.: Mar. 6, 2012).

- NTSB archives its safety recommendations in a publicly available database, including details of the implementation status of each recommendation it has made.

Disseminate Lessons

A critical step in any lessons-learned process is the sharing and disseminating of the knowledge gained. Agencies can disseminate lessons through many venues, such as briefings, bulletins, reports, emails, websites, database entries, the revision of work processes or procedures, and training. Lessons can be "pushed," or automatically delivered to a user, or "pulled," where a user searches for them. Lessons can also be disseminated with an assigned priority descriptor, which denotes the risk, immediacy, and urgency of the lessons-learned content. Examples of agencies using the dissemination and sharing practice include the following:

- As mentioned, Knowledge from the Field disseminates lessons by sending videos to all regional security officers. The videos summarize attacks and lessons learned using actual video, on-site reenactments, and interviews with witnesses.
- The Israeli Security Agency conducts debriefings with domestic security personnel across the government after incidents and relays the results of those debriefings to all overseas embassies and consulates.
- The Los Angeles Police Department produces a formal document after a critical incident that captures lessons learned and best practices that the department would like to sustain or improve. The department disseminates this document to its units for use in planning, preparing, and coordinating exercises.

Management Decision to Invest Resources

As part of the lessons-learned process, management must decide whether to invest resources to apply particular lessons. Under a benefit-cost analysis, some recommendations coming out of the lessons-learned process may simply be too costly to implement. Or it may be that the lesson learned was very specific to the particular circumstances of the incident and does not have wide applicability or a likelihood of future incidence. Examples of this step of a lessons-learned process include the following:

- Bureau of Diplomatic Services officials said that senior management is often engaged to determine where resources should be directed, in addition to considering the relevance of long-term training changes.

For example, the officials consider whether the circumstances around an incident are applicable not only today, but likely in the future as well.

- According to District of Columbia Metropolitan Police Department officials, after deriving lessons from incidents, management decides if, and the extent to which, changes in policy or procedures are needed. For example, the Police Department can implement lessons through general orders that support a change in policy or through changes in training that all units must apply to their operations.

Observe Change in Behavior

The seventh practice that agencies used will not necessarily be a step resulting from every lesson identified. As was shown in figure 1, this step is dependent on the prior step concerning management decisions about whether to take corrective action. If a decision is made to take action, then some agencies undertook subsequent action to observe that the change in behavior actually did occur and verify that the change had the desired effect. Observing changes in behavior after applying lessons requires additional information to validate the change resulted from the lesson. The following examples illustrate how law enforcement agencies use lessons to change the way they approach security incidents.

- To evaluate how lessons learned are applied, the Israeli Security Agency conducts drills to determine which changes work and which do not, communicate that information to its offices, and make necessary adjustments to physical security standards or procedures.

- The Greek police have learned from observing past demonstrations that it is important to provide an open route for people who want to leave. This has allowed demonstrators to more quickly and easily disperse.

Evaluate Effectiveness

As was shown in figure 1, the practice evaluating effectiveness is an ongoing part of the lessons-learned process. It involves assessing or measuring the performance of all steps in the process to seek continual improvement of the process as a whole. Overall, evaluating the effectiveness of a lessons-learned process involves weighing the use of resources against the desired results. Examples of agencies that evaluated the effectiveness of their physical security efforts include the following:

- Israel installed a system of 320 networked cameras to monitor activity in Jerusalem's Old City. The Israeli Police Department evaluated the effectiveness of the cameras through changes in the crime rate in the Old City, which dropped by 80 percent after the cameras were installed, according to Israeli authorities.

- The Bureau of Diplomatic Services is currently responding to recommendations we made in our June 2011 report[5] to measure the performance of its Knowledge from the Field effort, according to Bureau officials.

ISC Employs Some Practices and Is Beginning to Develop a Lessons-Learned Process

ISC Uses Some Lessons-Learned Practices

ISC currently does not have a systematic, comprehensive lessons-learned process for physical security. However, ISC officials cited a number of current initiatives that could support a more comprehensive lessons-learned effort.

- Updating physical security standards. According to ISC officials, ISC's process for updating its physical security standards includes collecting and analyzing information from past incidents to determine whether current countermeasures are consistent with the latest threats. In 2010, ISC established the *Design-Basis Threat* report, which is updated twice a year to identify threats and support the periodic updating of ISC's security standard.

- Subcommittees and working groups. ISC's subcommittees and working groups, which are comprised of volunteers from member agencies, help the agency capture and disseminate lessons learned and best practices. For example, the Countermeasures Subcommittee

[5]GAO, *Diplomatic Security: Expanded Missions and Inadequate Facilities Pose Critical Challenges to Training Efforts*, GAO-11-460, (Washington, D.C.: June 1, 2011).

oversees the development of security criteria and associated countermeasures necessary to mitigate the undesirable events as identified in the *Design-Basis Threat* report.

- Guidelines and Sharing of Best Practices. In recent years, ISC officials said that ISC has produced several guidelines for its members in an effort to capture and disseminate best practices on various topics that include physical security. For example, ISC produced a best practices guide for agencies to understand and mitigate risks posed by package bombs and other mail-based threats.

- Quarterly Meetings and Classified Briefings. ISC provides forums for its members to collect and disseminate physical security information and best practices through its quarterly meetings and annual classified briefings. ISC officials stated that regular contact with member agencies has promoted interagency coordination. During these meetings, participants often share physical security best practices and discuss emerging technologies. For example, at a recent briefing that we attended, the Bureau of Diplomatic Security provided physical security lessons learned from major incidents and threats occurring overseas.

- Homeland Security Information Network. ISC uses the Homeland Security Information Network (HSIN)[6] for archiving and sharing information. ISC has directed agencies to use HSIN to identify and share information, including physical security lessons. In general, federal officials said that HSIN was helpful in providing lessons learned from past incidents and other information. For example, one agency official stated that when an incident occurs, HSIN is used to identify after-action reports of the incident and any available physical security lessons learned.

Although these efforts by ISC relate to lessons learned, they are fragmented and uncoordinated. ISC officials said that ISC relies on

[6]The Department of Homeland Security is responsible for coordinating the federal government's homeland security communications with all levels of government – including state and local. In support of this mission, the department deployed and has been making improvements to HSIN as part of its goal to establish an infrastructure for sharing homeland security information.

agencies to volunteer their lessons for the benefit of others and that valuable lessons can be missed if an agency does not take the initiative.

ISC Is Developing a Lessons-Learned Process, but Whether It Can Be Implemented Is Unclear

In response to a February 2012 request from the Internal Revenue Service, ISC initiated a working group to explore the idea of creating a systematic, governmentwide lessons-learned process for physical security. ISC supports this effort because lessons from specific events or projects are not being shared to the fullest extent possible among the membership. In implementing a structured lessons-learned process, agency officials believe that the information collected would provide physical security information to federal facilities that would assist them in protecting against, responding to, and recovering from terrorist attacks, natural disasters, criminal activities, and other emergencies at federal facilities. The Lessons Learned and Best Practices Working Group, which consists of volunteer representatives from a number of federal agencies, had its first planning meeting in April 2012. The working group has established the following objectives:

- develop a charter accepted by all working group members and approved by the ISC Steering Committee,[7]
- establish an information sharing forum for the ISC membership,
- develop a process to deliver lessons learned and shared information to the full ISC membership, and
- develop a methodology to analyze potential items as a security "best practice" for approval by the Steering Committee.

The working group is a first step toward establishing a more deliberate lessons-learned process, but it remains at its early stages. It is not clear if the new program will include all of the practices that we have identified within a lessons-learned process. Developing a lessons-learned process for the security of federal facilities that does not incorporate all eight practices, as appropriate, could result in a less effective ISC lessons-learned effort and fail to maximize the value of the lessons learned to the ISC's membership.

[7]The ISC Steering Committee provides input to the Chair and Executive Director on priorities and project plans, as well as the operational impact of proposed initiatives to the security of federal facilities.

In developing a process to disseminate lessons learned governmentwide through its membership, an important issue for ISC is the unique, interagency makeup of its organization. The value of a lessons-learned effort led by ISC is the ability to take the lessons from an incident that affected one agency and share that knowledge broadly among many agencies so that all may benefit and federal facilities across the government may become more secure. Therefore, the authority of ISC to require their participation in sharing lessons is important to the effectiveness of ISC's effort. The Executive Order establishing ISC states that "each executive agency and department shall cooperate and comply with the policies and recommendations of the Committee." Agencies, however, are not sharing information with each other and ISC to the fullest extent possible. According to ISC officials, the committee serves at the will of the various agencies on which it relies for resources and support to accomplish its mission. ISC officials stated that they cannot force members to comply with its policies and recommendations. One possible option for clarifying ISC's authority is that the President could make clear that agencies are required to comply with ISC's policies and recommendations under the existing Executive Order. Another possible option would be for the Congress to provide ISC with statutory authority to carry out its policies and recommendations. A bill pending in the Congress, the Supporting Employee Competency and Updating Readiness Enhancements for Facilities (SECURE Facilities) Act of 2011,[8] would enact into law that "each agency shall cooperate and comply with [ISC's] polices, standards, and determinations." The bill would also require ISC to propose regulations to "establish risk-based performance standards for the security of Federal facilities," among other things. ISC officials stated that the bill would provide the statutory authority to compel agencies to comply with its policies, which could help it implement a systematic lessons-learned process for physical security.

[8] S. 772, 112th Cong. (2011). The purpose of this bill is to protect federal employees and visitors, improve the security of federal facilities, and authorize and modernize the Federal Protective Service.

Agencies Have Mitigated Some Challenges to Establishing a Governmentwide Lessons-Learned Process

Law enforcement agency officials we interviewed cited challenges specific to implementing a successful governmentwide lessons-learned process for physical security, including the need to (1) create a culture that encourages information sharing, (2) address the concerns about safeguarding sensitive security information, (3) determine how to disseminate lessons in a timely and formalized manner, and (4) overcome the constraints of limited human and financial resources. Agencies we met with had found ways to mitigate these challenges using strategies consistent with a lessons-learned process.

Create a Culture that Encourages Information Sharing

Organizational culture may be defined as the underlying assumptions, beliefs, values, attitudes, and expectations shared by an organization's members. Law enforcement agencies we interviewed cited cultural challenges to implementing a governmentwide lessons-learned process for physical security—intolerance for mistakes, lack of time, and questioning the benefits of lessons learned. However, agencies with experience using lessons-learned practices offered strategies that could help mitigate those challenges.

Intolerance for Mistakes

The culture of an organization could include an unwillingness to openly discuss mistakes or share those mistakes across organizational lines. It might also direct blame on those willing to bring problems forward. Several agency officials we interviewed said that they are reluctant to share negative lessons for fear that they might be viewed as incompetent or admitting failure. One police department official we interviewed stated that ego was the main barrier, adding that too often agency officials think that if they do something "wrong" or "bad," they do not want everyone to know about their mistakes. An official with the Bureau of Diplomatic Security stated that a structured lessons-learned process could face resistance if it highlights the mistakes of an agency or employee.

Our previous work and the work of the Center for Army Lessons Learned, along with Italian officials with whom we spoke, identified senior management as a way to help mitigate reluctance within an agency to share possibly embarrassing lessons. Senior management can promote openness and the strategic value in using knowledge, and communicate to their employees that sharing knowledge is critical to their success. Specifically, the Italian officials noted that an effective lessons-learned effort should also collect information on what is working well and best practices. The Center for Army Lessons Learned also pointed out that agency managers can reinforce their commitment to open communication

by integrating effective information sharing into staff performance expectations and appraisals.

Time Constraints

Some law enforcement officials with whom we spoke said that there is a lack of time for sharing lessons learned. Consequently, they said that knowledge-sharing activities can be seen as an additional burden on top of an already heavy workload. A General Services Administration official stated that department and agency representatives to ISC already have ISC responsibilities in addition to their own agency responsibilities, so forming yet another working group would be taxing to many agency representatives. Greek law enforcement officials noted that they were dealing with an increasing pace of demonstrations outside government buildings, which has placed time constraints on the ability to do other tasks including identifying lessons learned from the last demonstration.

Officials from the Center for Army Lessons Learned and the Israeli Security Agency said that benefits of an effective lessons-learned process can convince people to prioritize it. The Center for Army Lessons Learned officials said that agencies should not view lessons learned as different from normal activities and that lessons-learned practices should be embedded into the agency programs that they are meant to improve. For example, Bureau of Diplomatic Security officials said that the bureau tries to increase involvement in the Knowledge from the Field program and use resources efficiently by using existing networks and procedures in developing its lessons-learned videos. For example, the program relies on State Department officials in the field to nominate lessons, uses the existing after-action reports and event videos, and integrates the lessons into the existing training classes for security officers.

Some Question the Benefits of a Formal Lessons-Learned Process

Some law enforcement officials we interviewed stated that there are not enough physical security incidents to warrant the creation of a governmentwide lessons-learned process. A Smithsonian Institution Office of Protection Services official stated that given the limited number of major security incidents compared to the large number of buildings throughout the federal government, there does not appear to be a problem with the current practices that federal agencies use to learn from those incidents. Officials from the U.S. Marshals Service stated that establishing a governmentwide lessons-learned process would be problematic because every building has unique security requirements which limit the benefits of sharing information.

Conversely, Bureau of Diplomatic Security officials said that the low number of incidents increases the need to share lessons from the

incidents that occur. The officials said that people learn through experience and, due to the low number of incidents, the lessons learned by others may be the closest many federal security officials come to direct experience. For example, State Department officials said that Knowledge from the Field is supported by the Bureau of Diplomatic Security's institutional willingness and responsibility to learn from mistakes. State Department officials said that they take efforts to use actual incident video, recordings, and interviews to make the lessons more compelling and as real as possible for those not actually involved. Similarly, NTSB holds public meetings with eyewitness accounts, computer generated simulations, and accident photos to relate the importance of the lessons NTSB is attempting to convey.

Concerns about Safeguarding Sensitive Information

Officials from law enforcement agencies and organizations with experience in using lessons-learned practices stated that an area of particular concern in physical security is the protection of sensitive information maintained by federal agencies. Sensitive data can include details of security countermeasures, information pertaining to criminal investigations, and data regarding emergency preparedness. Several agency officials expressed concerns about broadly sharing sensitive information out of fear the information would be compromised. For example, a U.S. Marshals Service official stated that he was particularly concerned about sensitive information being disseminated too widely because people could instead use lessons learned as a blueprint for future attacks.

ISC officials said that the fear of law enforcement information getting into the wrong hands is legitimate, but that ISC's current information-sharing system is configured to handle access to information of different security levels. Officials from the Israeli National Police also said that sensitive information must be protected, but that lessons learned are valuable and information must be shared appropriately and with appropriate access. Officials from the Center for Army Lessons Learned said that the Army faces this same challenge but indicated that placing excessive security restrictions on lessons-learned information reduces dissemination, defeating the purpose of a lessons-learned process. They said that they have worked to redact certain information, such as the methods used in collecting the information or personal identifiers, so that sensitive information is protected but the information disseminated is still useful.

Slow Dissemination and Reliance on Informal Networks

According to some law enforcement officials with whom we spoke, there is a concern that physical security lessons would be disseminated too slowly using a systematic lessons-learned process. For example, U.S. Marshals Service officials said they are concerned that formally collecting and analyzing data with the intent to produce lessons learned would be time consuming and could take too long to be disseminated. As a result, officials from several international and domestic law enforcement agencies said that they prefer informal networks for capturing information quickly. However, one Justice Protective Service official acknowledged that while informal mechanisms are quicker than structured mechanisms, the information is often anecdotal and the recipients of the information must be careful that the information is reliable.

Setting expectations and staggering the release of lessons-learned information can mitigate this challenge. According to Center for Army Lessons Learned officials, the risk in rapidly sharing information is that you fail to conduct a thorough analysis and validate that you are drawing the correct lessons. The Army officials recommended creating timelines for sharing information that are tied to the urgency of the information, so that the most critical information gets out first. For example, according to the Center for Army Lessons Learned, an “immediate” requirement to share a particular lesson, that if not shared, could result in the injury or death of a soldier. However, once rapidly shared, information should continue to be analyzed and eventually be formally vetted, archived, and become a part of the issues-resolution process. For example, NTSB officials said that NTSB may issue a safety recommendation fairly quickly and well before it completes and issues its final accident-investigation report. As for sharing information via informal networks, interacting informally with other agency officials is a valid method of sharing information, but it is not necessarily the most effective way. Relying solely on informal networks for capturing lessons is problematic because personal networks can dissolve, e.g., through attrition or retirement, and informal information sharing does not ensure everyone is benefiting from the lessons that are gleaned. In addition, informal exchanges do not generally allow the information to be validated.

Limited Human and Financial Resources

Some agencies we interviewed—such as the Justice Protective Service, U.S. Marshals Service, and the General Services Administration—cited the lack of human and financial resources as a barrier to establishing a structured lessons-learned process for real property security. Officials from the U.S. Holocaust Memorial Museum and the Smithsonian Institution noted that ISC could be the appropriate federal body to run

such a governmentwide lessons-learned effort. However, the Smithsonian official also said that implementing a formal, governmentwide lessons-learned process would require ISC to allocate sufficient resources. The Holocaust Museum official suggested that if such a process were established, federal funds should be appropriated to support it.

Because establishing a structured lessons-learned process can take several years, Center for Army Lessons Learned officials stated that organizations should start small, do what is possible with the resources they have, build gradually, and leverage existing structures and practices instead of creating an entirely new, separate process. Also, previous GAO work and the work of the Center for Army Lessons Learned emphasize that senior leadership need to be actively engaged in lessons-learned efforts and prioritize resources to ensure that changes happen and lessons are actually learned and disseminated.

Conclusions

Although attacks on federal buildings and public spaces remain rare, recent attacks show the continuing potential for violent acts. ISC has some of the practices in place to identify and apply lessons learned for physical security, but it does not have in place a systematic, structured lessons-learned process. Without a more structured, governmentwide effort, attackers could continue to exploit the same weaknesses in government security. Recognizing this, ISC has taken the important step of initiating a structured lessons-learned process for physical security, starting with its working group, but that effort is just beginning. It is unclear the extent to which ISC's new effort will apply each of the practices of a lessons-learned process identified in our report. Without implementing each of the eight practices of a lessons-learned process, as appropriate, ISC's effort might not reach its full potential and will run the risk of lacking relevance within the law enforcement community it seeks to assist. In addition, because of ISC's limited resources, it will be important to build its lessons-learned process gradually and leverage its existing practices.

Once ISC establishes its lesson-learned process, it will be important for all of its member agencies to participate. However, ISC currently relies on agencies to take the initiative to promote their lessons to others—something that does not always happen due to the guarded culture of the physical security community. As a result, ISC officials have questioned if ISC has sufficient authority to implement an effective lessons-learned process since it currently operates under an Executive Order, as opposed to pursuant to a statutory requirement. If ISC cannot encourage or compel

all relevant agencies to learn and share lessons, its effort could miss important lessons that could help protect federal buildings and save lives.

Recommendations for Executive Action

To improve the federal government's ability to learn from and disseminate physical security lessons, we recommend that the Secretary of Homeland Security direct ISC to:

- Develop a lessons-learned process for physical security that will (1) leverage the lessons-learned practices it already employs and (2) incorporate the full range of lessons-learned practices identified in our report.
- Determine, as it develops a lessons-learned process, whether Executive Order 12977 provides sufficient authority to effectively support a systematic, governmentwide lessons-learned effort. If ISC determines that it does not have sufficient authority, it should then determine the best course of action to seek the needed authority.

Agency Comments

We provided a draft of this report to DHS, and the departments of Defense, the Interior, Justice, and State; the General Services Administration; NTSB; the Smithsonian Institution; and the U.S. Holocaust Memorial Museum for review and comment. DHS agreed with our recommendations. See appendix II for a copy of DHS's comments. Separately, DHS offered technical comments, which we incorporated where appropriate. All of the other agencies stated that they had no comments on the draft report.

We are sending copies of this report to the Secretaries of Defense, Homeland Security, the Interior, State, and the Smithsonian Institution; the U.S. Attorney General, the Administrator of the General Services Administration; the Chair of NTSB; the Executive Director of the U. S. Holocaust Memorial Museum; and interested congressional committees. The report is also available at no charge on GAO's Web site at http://www.gao.gov.

If you or your staff have any questions concerning 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. GAO staff who made major contributions to this report are listed in appendix III.

Mark L. Goldstein
Director, Physical Infrastructure Issues

Appendix I: Scope and Methodology

Our overall scope was to review lessons-learned practices and their applicability to the protection of federal facilities and public spaces. To accomplish this work, we identified a lessons-learned process that could be applied to the protection of federal facilities and public spaces. To accomplish this, we primarily used our previous work and a report from the Center for Army Lessons Learned.[1] We selected the process descriptions in these two reports based on the following factors:

- GAO and the Center for Army Lessons Learned developed their process descriptions based on the breadth of their collective research, interviews, and experience, as well as the experience of the organizations they reviewed.
- Together GAO and the Center for Army Lessons Learned included lessons-learned practices of the government and private sector.
- The GAO and Center for Army Lessons Learned reports, although published 10 years apart, used consistent language in defining a lessons-learned process.
- The Army and law enforcement and security agencies have common general responsibilities to protect employees and the public from violent threats and incidents.

We reviewed these two process descriptions and combined them with information from our reviews of relevant literature and early interviews with agencies to identify eight individual practices for identifying and applying lessons learned. We combined and ordered these practices to develop an overall, eight-step, lessons-learned process—a systematic means for agencies to learn from an event and make decisions about when and how to use that knowledge to change behavior.

To determine how law enforcement and security officials apply lessons-learned practices to the protection of federal facilities and public spaces, we interviewed officials knowledgeable of their agencies' policies and procedures for the physical security of the facilities they protect. We

[1]GAO, *NASA: Better Mechanisms Needed for Sharing Lessons Learned*, GAO-02-195 (Washington, D.C.: Jan. 30, 2002); and Center for Army Lessons Learned, *Establishing a Lesson Learned Program: Observations, Insights, and Lessons* (Fort Leavenworth, Kansas: June 2011).

judgmentally selected 7 federal law enforcement and physical security agencies that secure and protect government facilities and spaces that allow broad public access or because they recently faced attacks:

- Bureau of Diplomatic Security, Department of State, for overseas embassies and consulates and domestic passport offices;
- Federal Protective Service, Department of Homeland Security, for federal courthouses and federal government agencies;
- Office of Protection Services, Smithsonian Institution, for the Smithsonian museums;
- Protection Services, U.S. Holocaust Memorial Museum;
- U.S. Marshals Service, Department of Justice, for the federal courthouses;
- U.S. Park Police, National Park Service, for the national parks and icons; and
- U.S. Park Rangers, National Park Service, also for national parks and icons.

We interviewed two other federal agencies that protect facilities with less public access—the Federal Bureau of Investigation and the Justice Protective Service of the Department of Justice. We also interviewed officials and obtained documents from the National Transportation Safety Board (NTSB). We included NTSB in our review because its mission and processes involve the practices of the lessons-learned processes we identified. NTSB implements lessons-learned practices by investigating accidents, determining their causes, issuing safety recommendations, and conducting safety studies.

We judgmentally selected 5 domestic and 5 foreign cites based on interviews with law enforcement and security officials because they draw large groups of tourists to government facilities, public spaces, or to private attractions. We interviewed 8 local and 12 foreign police departments and security agencies within these 10 cities.

- Athens and Thessaloniki, Greece: Greek Police Force, VIP Protection and Security Service, Parliament Security, and Combined Operation Center;
- Jerusalem, Israel: Israeli Security Agency, Security Division of the Ministry of Tourism, Israeli National Police, and Knesset Security Office;
- Las Vegas, Nevada: Las Vegas Metropolitan Police Department, Las Vegas City Marshals, and Southern Nevada Counter-Terrorism Center;

- Los Angeles, California: Los Angeles Police Department;
- New York, New York: New York City Police Department;
- Rome, Italy: Rome Police, Department of Public Security of the Ministry of Interior, and the Physical Security Office of the Italian Senate;
- St. Louis, Missouri: St. Louis Metropolitan Police Department;
- Vatican City: Security Office of the Vatican City; and
- Washington, D.C.: District of Columbia Metropolitan Police Department and Protective Services Police Department.

We interviewed officials from 4 federal agencies with responsibilities for developing physical security standards and guides:

- Interagency Security Committee (ISC): ISC produces *Physical Security Criteria for Federal Facilities*, which establishes a baseline set of physical security measures to be applied to all federal facilities and provides a framework for the customization of security measures to address unique risks at a facility;

- General Services Administration (GSA): As the federal government's landlord, GSA designs, builds, manages, and, with the help of the Federal Protective Service, safeguards buildings to support the needs of other federal agencies. It published *The Site Security Design Guide*, which establishes the principles, explores the various elements, and lays out the process that security professionals, designers, and project and facility managers should follow in designing site security at any federal project.

- Overseas Security Policy Board (OSPB): As part of the Diplomatic Security Bureau, OSPB establishes the security standards and policies for all new embassy compounds, new office buildings, newly acquired buildings, existing office buildings, and commercial office space that are intended for the conduct of diplomacy, whether acquired by purchase or lease.

- Technical Support Working Group (TSWG): The Physical Security Subgroup of the Department of Defense's TSWG identifies the physical security requirements of federal, state and local agencies, both within the United States and abroad, develops technologies to protect their personnel and property from terrorist attacks, and manages projects to develop prototype hardware, software, and systems for technical and operational evaluation by user agencies. We also reviewed the Department of Defense's *Unified Facilities*

Criteria (UFC) documents, which provide planning, design, construction, sustainment, restoration, and modernization criteria, and apply to the military departments, defense agencies, and the Department of Defense field activities.

To determine the actions that ISC has taken to learn lessons from attacks on federal facilities, we interviewed officials from ISC and some of its member agencies, obtained and analyzed documents, and attended two quarterly meetings held for its member agencies. Also, some of the officials we interviewed from other federal agencies also represented their agencies for ISC activities. The documents we analyzed and discussed with ISC officials included the *Physical Security Criteria for Federal Facilities* standards document and the *Design-Basis Threat* report, which creates a profile of the type, composition, and capabilities of adversaries; and is designed to correlate with the countermeasures contained in the *Physical Security Criteria for Federal Facilities*.

To determine the challenges that law enforcement agencies face for the development of a governmentwide lessons-learned process for real property security, we visited or interviewed officials about this issue from the aforementioned federal, local, and foreign government agencies in the domestic and international cities described above. To determine what strategies could mitigate challenges to developing a governmentwide lessons-learned process for real property security, we analyzed the previously mentioned GAO and Center for Army Lessons Learned reports. These two agencies discussed the challenges and barriers that organizations could face in implementing lessons-learned processes, and the knowledge management principles and actions that could mitigate the challenges and barriers. We also analyzed the results of all our interviews with the federal, local, and foreign government agencies to glean challenges and barriers and mitigation elements specific to the law enforcement and physical security environment.

Appendix II: Comments from the Department of Homeland Security

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

Homeland Security

August 24, 2012

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

Re: Draft Report GAO-12-901, "FEDERAL REAL PROPERTY SECURITY: Interagency Security Committee Should Implement A Lessons Learned Process"

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 GAO's highlighting the importance of securing Federal facilities to protect employees and the visiting public, as well as the essential role the Interagency Security Committee (ISC) plays in facilitating enhanced security. The ISC has a number of current initiatives that can support a more comprehensive lessons learned effort, to include updating physical security standards, subcommittees and working groups, guidelines and sharing best practices, quarterly meetings and classified briefings, and the Homeland Security Information Network. The ISC has taken the important step of initiating a structured lessons learned process, starting with the formation of a Lessons Learned and Best Practices working group. Providing specific details regarding the Working Group at this point would be premature because development of the working group charter is underway.

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

Recommendation 1: Develop a lessons learned process for physical security that will (1) leverage the lessons learned practices it already employs and (2) incorporate the full range of lessons learned practices identified in the report.

Response: Concur. As previously mentioned, the ISC has formed a Lessons Learned and Best Practices working group. The Working Group is in the beginning stages and currently developing a charter that lays out the vision and mission, roles and responsibilities, and expectations of the Working Group, to name a few elements of the charter. During the formulation of the Working Group charter, the ISC will take the GAO's report and recommendation into consideration.

Recommendation 2: Determine, as it develops a lessons learned process, whether Executive Order 12977 provides sufficient authority to effectively support a systematic, government-wide lessons learned effort. If ISC determines that it does not have sufficient authority, it should then determine the best course of action to seek the needed authority.

Response: Concur. Executive Order 12977 states that "each executive Agency and Department shall cooperate and comply with the policies and recommendations of the Committee issued pursuant to this order." The ISC has successfully supported the development of standards for Federal building security in accordance with the Executive Order and will be able to support the development of a lessons learned process. All standards developed by the ISC are reviewed and approved by the primary membership thereby ensuring concurrence by all committee members.

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

2

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contact

Mark L. Goldstein (202) 512-2834 or goldsteinm@gao.gov

Staff Acknowledgments

In addition to the contact named above, Keith Cunningham (Assistant Director), Antoine Clark, Colin Fallon, Sam Hinojosa, David Hooper, Sara Ann Moessbauer, Faye Morrison, and Nalylee Padilla.