Interagency Security Committee
End of Year Report
2006

Introduction

On June 28, 1995, the Department of Justice (DOJ) issued the *Vulnerability Assessment of Federal Facilities*. One recommendation of the report was to establish an Interagency Security Committee (ISC) to address government-wide security concerns. On October 19, 1995, the President signed Executive Order (EO) 12977 creating the ISC.

With the establishment of the Department of Homeland Security (DHS), the ISC was transferred to DHS; however, the ISC's primary duties and responsibilities remained unchanged:

- Establish policies for the security in, and protection of nonmilitary federal facilities
- Develop and evaluate security standards for federal facilities; develop a strategy for ensuring compliance with such standards; and oversee the implementation of appropriate security measures in federal facilities, and
- Take such actions as may be necessary to enhance the quality and effectiveness of security and protection of federal facilities

In 2005, the responsibility to Chair the ISC was delegated to the DHS Chief Security Officer. Currently the ISC has 21 primary members designated by EO and 19 associate members. Associate members are those who have expressed a desire to participate in ISC meetings and assist in its activities and working groups. The Chair is assisted by an Executive Director and a Steering Group that advises on program issues and priorities.

The ISC initiatives are governed by the following vision, mission, and objectives:

Vision:

A collaborative organization that provides leadership to the nonmilitary federal community supporting physical security programs that are comprehensive and risk based.

Mission:

The Interagency Security Committee enhances the security in, and protection of nonmilitary buildings and facilities in the United States occupied by federal employees and other personnel. It establishes physical security policies and standards, promotes key management practices, and engages in other activities that facilitate the mitigation of threats to the workplace, employees, and the visiting public.

Objectives:

- Improve Security Program Management.
- Enhance Guidance and Standards for Security Operations.
- Improve Coordination of Security and Protection Initiatives.

ISC Accomplishments in 2006

ISC Planning Conference and Action Plan

In September 2006 the ISC conducted its first biennial planning conference. The conference was the culmination of several months of effort beginning with a survey sent to all ISC members soliciting their views on ISC priorities. Survey responses were followed up with member interviews in which additional priority suggestions were identified. Government Accountability Office (GAO) audit reports on the ISC were also incorporated into the planning conference deliberations.

The conference was held at the Federal Deposit Insurance Corporation (FDIC) training facility in Arlington, VA. Attendees included ISC members and representatives from the Office of Management and Budget (OMB). During the conference ISC members agreed on the ISC's vision, mission, and objectives and discussed over 30 potential tasks for enhancing federal facility security. Consensus was reached on completing five in-progress initiatives, four addressed key management practices for security managers, as recommended by the GAO. Results of the planning conference were documented in a 2007-2008 ISC Action Plan.

Safe Mail Handling Guidance

In September 2006, the ISC issued *Best Practices for Safe Mail Handling*. The report addresses issues associated with suspicious mail and recommends measures agencies may implement to safely handle and deliver mail to personnel. The U.S. Postal Service led the effort, assisted by Federal Deposit Insurance Corporation (FDIC), General Services Administration (GSA), DHS, and the Department of Transportation (DOT).

ISC Standard Operating Procedures

In December 2006, the ISC revised its Standard Operating Procedures (SOP). The new SOP identified ISC Steering Group and Working Group responsibilities, voting processes, and internal procedures to promote more efficient decision making, and to document work product development and approval processes.

HSPD-7 Support

During 2006, the ISC was tasked by Office of Management and Budget (OMB) to review the physical security portion of federal agencies' National Critical Infrastructure Plans, as required by Homeland Security Presidential Directive (HSPD) -7, *Critical Infrastructure Identification, Prioritization, and Protection*. Twenty-two Cabinet-level departments and agencies submitted critical infrastructure and key resources protection plans. The ISC, in conjunction with DHS's Federal Protective Service (FPS), conducted a review and

comparative analysis of all plans. Results, which were submitted to OMB, provided information on security gaps and resource requirements.

HSPD-12 Support

HSPD-12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, mandates a government-wide standard for secure and reliable forms of identification for federal employees and contractors. The Department of Commerce (DOC) was designated lead-agency for this task. Because of the impact on all federal agencies the ISC became actively involved in an oversight and support role.

National Infrastructure Protection Plan Support

The Chief of the Government Facilities Sector (GFS) of the National Infrastructure Protection Plan (NIPP) initiative addressed the ISC at the May 2006 meeting. The ISC became a security partner with the Government Coordinating Council (GCC) of the GFS to develop plans and policies for more secure government facilities at all levels. The ISC provides support and collaboration to the GCC for critical infrastructure/key resources protection activities consistent with existing authorities, and shares security-related best practices. ISC staff and members provided vital input on the *National Infrastructure Protection Plan* and the *Government Facilities Sector-Specific Plan* intended to prevent, deter, neutralize and mitigate the effects of efforts by terrorists to destroy, incapacitate, or exploit the nation's critical infrastructure or key resources.

Membership

In 2006, the ISC's associate membership increased to nineteen with the addition of The Smithsonian Institution. The Smithsonian's membership request was approved by the ISC Chair on October 31, 2006. The Smithsonian is a welcome addition and will bring unique experience and expertise to the benefit of all members.

Working Groups In-Progress

Security Standards for Existing Buildings

In January 2006, ISC members voted to establish a working group to revise the 1995 DOJ *Vulnerability Assessment of Federal Facilities* report. The working group is chaired by DOJ, with members from the Environmental Protection Agency (EPA), FDIC, GSA, DHS, Nuclear Regulatory Commission (NRC), The Department of Treasury (Treasury), and the US Courts. The new document will focus on three areas: 1.) enhanced guidance to determine appropriate facility security levels; 2.) updated baseline physical security standards for each security level; and 3.) new guidance for adjusting baseline security standards based on site-specific threats and vulnerabilities. Much from the 1995 DOJ report will remain, to include security level designations and security levels determinants. New guidance material will include criticality and other threat factors affecting the final facility security level determination. This new document will be a companion to the 2004 *ISC Design Criteria for New Federal Office Buildings and Major Modernization Projects*, and the 2005 *ISC Security Standards for Leased Space*

Physical Security Standards for Child Care Facilities

To ensure physical security considerations become an integral part of the concept development, design, and construction of child care centers in federal facilities, an ISC working group was established to develop an amendment to the *ISC Security Design Criteria for New Federal Office Buildings and Major Modernization Projects.*

Physical Security Standards for Land Ports of Entry

DHS/Customs and Border Protection (CBP) is revising the security standards for land ports of entry (LPOE). The LPOE mission involves the inspection of travelers entering the United States, revenue collection, and preventing the entry of illegal aliens, injurious plants, animal pests, and human and animal diseases. The revised CBP *Land Border Design Guide* will be an addendum to the *ISC Security Design Criteria for New Federal Office Buildings and Major Modernization Projects*. The document will identify design criteria elements that are appropriate to the unique mission and operations of LPOE. CBP's Office of Internal Affairs is leading this initiative, with assistance from GSA, ISC staff, and other CBP components.

Law Enforcement Access to Federal Facilities

In 2001, the ISC Chair issued a policy on law enforcement access to federal facilities. The policy allows access to armed law enforcement personnel only while on official business. In 2006, a working group was chartered to address unresolved issues that had surfaced concerning the policy. The group's intent is to achieve consensus and closure on this initiative in 2007.

HSPD-12 Migration Strategy

In October 2006, the ISC became active in the effort to meet and standardize the physical security requirements of HSPD-12, and facilitate a consistent and coordinated approach in the use of personal identity verification (PIV) cards. The development of an effective and efficient strategy for the use of current and future physical access control systems is a critical element of HSPD-12. This working group is chaired by DOC with assistance and input from all ISC members.

Initiatives for 2007-2008

Key Management Practice: Use of Performance Measures and Testing

In response to a GAO audit recommendation, the ISC will issue a policy and guidance document requiring the use of performance measurement and testing to assess the effectiveness of physical security programs. The guidance will define input, output, and outcome measures and discuss their use in evaluating program effectiveness, allocating resources, and providing accountability and recognition for security professionals. The ISC staff will lead a working group consisting of representatives from the National Infrastructure Protection Plan's Government Facilities Sector and Department of Defense (DOD). The target date for final issuance is July 2007.

Key Management Practice: Allocating Resources Using Risk Management

The ISC will address the application of risk management factors to determine appropriate resources to meet security requirements. Guidance will be developed to include identifying potential threats, assessing vulnerabilities, identifying the assets most critical to protect in terms of mission and significance, and evaluating mitigation alternatives for their effect on risk and cost. The objective is to produce guidance that is adopted by agencies and provided the foundation for an effective facility protection program. The working group is chaired by the Department of State (DOS) with assistance from DoD, Department of Education, Federal Bureau of Investigation (FBI), GSA, DHS/Infrastructure Protection, and Social Security Administration.

Key Management Practice: Strategic Management of Human Capital

This effort involves security specialist qualifications, standards, and performance. It includes coordination with the Office of Personnel Management (OPM) on specific job qualifications, training, and certification for government security specialists. Minimum requirements for contract security personnel will also be reviewed. The objective is to develop government-wide guidance to standardize/professionalize the security career field, to include standards for: continuing education and training; professional affiliations and accreditation; and consistency in position descriptions, duty titles, and job classifications. The working group established for this initiative includes the Department of Agriculture (USDA), Department of Labor (DOL), OPM, US Marshals Service (USMS), and the Department of Veterans Affairs (VA).

Key Management Practice: Leveraging Technology

The efficient and appropriate use of technology can reduce deficiencies identified in the risk management process. GAO report 05-49 suggested the ISC find cost-effective methods to address threats and vulnerabilities with new technologies. This working group will examine new technologies and how best to leverage their use in securing federal facilities as part of a risk management process. Factors will be considered are: benefit; purpose; const; and expected performance. DOD will lead this group with members from the FBI, DHS/Science and Technology (S&T), and the National Institute of Standards and Technology.

Guidance and Minimum Standards for Contract Guards

This effort will define the guard force functions as a threat countermeasure. It will contain guard post identification and staffing guidelines, and compare guard forces with other threat countermeasures to enable security professionals to more effectively integrate security systems. The document will also address the need for, and elements of a job task analysis for contract guard positions, and identify minimum program standards such as medical, physical, and training. The working group for this task will be led by DHS/FPS supported by the Department of Education, Environmental Protection Agency (EPA), GSA, Social Security Administration, and DOS.

ISC Guidance on Construction Standards for Shelter in Place Facilities

The development of guidance for construction standards for shelter in place facilities was determined to be a priority ISC initiative. The guidance will support preparedness objectives in the National Preparedness Goals for terrorist attacks and natural disasters. The working group will consider shelter design concepts and how design influences site location and the effect on safe ingress and egress. The objective for this initiative is to provide a broad vision on how a shelter should be designed for catastrophic events. DHS/Federal Emergency Management Agency will lead the working group with assistance from DOJ, GSA, OPM, Central Intelligence Agency, Department of Energy, and Department of Health and Human Services/Center for Disease Control.

ISC Marketing and Communications with Agencies and Security Partners

This ISC staff initiative is to develop a marketing plan for information sharing so agencies have a clear picture of the ISC and its products. This includes developing methods to advertise the ISC, educate government agencies on ISC responsibilities and capabilities, and communicate with ISC members and partners frequently and rapidly on pertinent security data and information. This initiative will be accomplished by the DHS ISC staff with assistance from other DHS sources and the US Postal Service.

Future Challenges

Many ISC duties and responsibilities are being addressed, but additional action is needed to: develop a strategy to ensure compliance with ISC standards; oversight of the implementation of security measures; and establishment of a federal security assets database. These additional actions are supported by GAO recommendations for improving physical security program management.

The current multi-dimensional threats of terrorism, crime, and workplace violence significantly complicate physical security operations. Because terrorist attacks in the United States have involved federal facilities, federal agencies and departments must proactively guard against attack while at the same time reconciling potential threats through the use of risk management. Collectively ISC membership is challenged to lead the development of federal security policies and standards, while individually ISC members must manage change within their own agency or department.

Conclusion

The ISC continues to make progress in achieving its objectives. The 2006 Planning Conference validated the ISC's commitment to addressing high priority issues confronting the federal physical security community. The new ISC standard operating procedures will make ISC working group activities and decision making more efficient and timely. The positive long-term benefits of the accomplishments made by the ISC during 2006 will have a significant impact on future efforts to improve security in, and the protection of federal facilities.