Written Testimony

of

Scott Breor

Associate Director, Security Programs

Infrastructure Security Division

Cybersecurity and Infrastructure Security Agency

US. Department of Homeland Security

Before the

U.S. House of Representatives,

Committee on Homeland Security

Subcommittee on Oversight, Management and Accountability

Regarding

Federal Building Security: Examining the Risk Assessment Process

September 22, 2022

Introduction

Chairman Correa, Ranking Member Meijer, and Members of the Subcommittee, my name is Scott Breor, and I am the Associate Director for Security Programs within the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency's (CISA) Infrastructure Security Division (ISD). I appreciate the opportunity to appear before you today to discuss the DHS's Interagency Security Committee's (ISC) role in the protection of federal buildings and its efforts to improve preparedness, in coordination with interagency partners.

The Interagency Security Committee and its Role in the Protection of Federal Facilities

The ISC was created in the wake of the April 19, 1995, bombing of the Alfred P. Murrah Federal Building in Oklahoma City, Oklahoma. The attack on that federal facility served as a national tragedy with the loss of 168 lives, including 19 children. To this day, the Oklahoma City attack remains the deadliest domestic terrorist attack on American soil in our history.

Following the Oklahoma City bombing, President Bill Clinton issued Executive Order (EO) 12977 to "enhance the quality and effectiveness of security in and the protection of buildings and nonmilitary federal facilities in the United States," and to create the ISC. DHS has chaired the ISC since March 2003, when, pursuant to EO 13286, the role of chair transferred from the General Services Administration (GSA) to DHS. DHS delegated this responsibility to CISA as a result of its role as the nation's risk advisor and its task to help secure critical infrastructure. CISA provides the leadership, management, and compliance monitoring necessary to meet the requirements of EO 12977. CISA's stewardship of the ISC ensures its work both supports and leverages state, local, territorial, and tribal organizations, as well as the private sector, all of whom are essential partners as we work to ensure the continued protection of federal facilities and assets across the nation and around the world.

Role of the Interagency Security Committee in Federal Facility Security

When the ISC was created in 1995, it consisted of the 21 members outlined in EO12977. Today, the ISC includes 66 members. In addition to Executive Branch agencies, the ISC includes representatives from outside the Executive Branch such as the United States Capitol Police and the Administrative Office of the United States Courts. Membership consists of departments and agencies whose headquarters are both inside and outside the National Capital Region. This collective security subject matter expertise allows the ISC to develop top-tier risk management resources and to coordinate interagency solutions to problems that cannot be solved by individual departments and agencies alone.

The ISC is a collaborative forum that carries out its work by, with, and through its members within a primary governance framework of subcommittees and working groups. The ISC's eight standing subcommittees guide the development of ISC policies and strategic initiatives. Additionally, the ISC establishes working groups, which are provisional, task-based bodies with clear objectives and defined deliverables.

EO 12977 gave the ISC three key responsibilities. These include:

- Establish policies for security in, and protection of, federal facilities;
- Develop and evaluate security standards and a strategy to ensure compliance; and
- Take necessary actions to enhance the quality and effectiveness of security and

protection of federal facilities.

The ISC fulfills these responsibilities through multiple lines of effort. The first is the Risk Management Process: An Interagency Security Committee Standard (RMP Standard). The RMP Standard provides an integrated, single source of physical security countermeasures and guidance on countermeasure customization for all nonmilitary federal facilities. ISC members created the RMP Standard to provide a common method for all federal facility security stakeholders; specifically owning and leasing organizations, security organizations and the members of departments and agencies that are tenants in federal facilities; to guide risk assessments of federal facilities in a standardized way and to help facilities owners identify levels of protection needed to mitigate that risk.

In addition to the core RMP Standard, the ISC produced and issued over 20 other products, including authoritative guidance on planning and response to an active shooter situation, a standard for prohibited items at federal facilities, and other best practices and guides. ISC guidance documents are distributed via department and agency member representatives and senior leaders within their organizations. Federal facility security stakeholders can also download the documents from the ISC web presence at CISA.gov. Each organization uses best practice documents and guides as a means to enhance the security of and protection of federal facilities, and those who visit or occupy them. A sample of these products include:

- Security Convergence: Achieving Integrated Security: An Interagency Security Committee Best Practice;
- Protecting Against the Threat of Unmanned Aircraft Systems (UAS): An Interagency Security Committee Best Practice;
- Facility Access Control: An Interagency Security Committee Best Practice;
- *Violence in the Federal Workplace: A Guide for Prevention and Response*;
- Facility Security Plan: An Interagency Security Committee Guide; and
- Planning and Response to an Active Shooter: An Interagency Security Committee Policy and Best Practices Guide.

ISC guidance is designed to be scalable and tailorable to the unique security environment and site-specific needs of the diverse membership of the ISC. Further, the ISC validates member risk assessment tools and training programs as meeting the RMP Standard. This helps build individual and organizational capability to successfully implement ISC guidance.

The ISC also monitors compliance with its policies and standards at the organizational and facility level. This includes providing federal facility stakeholders with the means to measure, report, and analyze compliance against a set of benchmarks using a web-based platform. The resulting data and analyses help departments and agencies focus their efforts and resources while providing feedback to the strategic direction of the ISC's work. Examples of areas where this valuable information has informed action include refining policy, developing training and other capacity building efforts, and developing automated support tools. The results of ISC compliance findings are briefed to the ISC Chair, and also made available to the relevant ISC member departments and agencies, to ensure necessary corrective actions are taken to enhance compliance with ISC policies and standards.

ISC Partnership with the Federal Protective Service

CISA, through its stewardship of the ISC, works with partners across government and the private sector to ensure our nation's federal facilities are protected against the threats of today. Two of the main drivers of threats to federal facilities are targeted violence and terrorism. As noted in the DHS National Terrorism Advisory System Bulletin, these threats are becoming more dynamic and complex—combatting these threats is and will remain a top priority for DHS. Within DHS, our partners at the Federal Protective Service (FPS) play a key role on the ISC. FPS actively contributes to seven of the ISC's eight standing subcommittees and all three operating working groups. The FPS also provides valuable leadership, chairing two of the eight subcommittees and one of the three working groups.

In addition to contributing to the collective work of the ISC, FPS provides security for facilities under GSA's jurisdiction, custody or control as well as numerous non-GSA federal properties throughout the country. As part of this responsibility, FPS conducts risk assessments to identify risk(s) and recommended security countermeasures to mitigate corresponding risk(s). In conducting these assessments, FPS uses a risk assessment tool that has been validated by the ISC, the Modified Infrastructure Survey Tool. Additionally, FPS's Physical Security Training Program located at the Federal Law Enforcement Training Centers has similarly been validated by the ISC. This training program trains FPS personnel on how to conduct a risk assessment using their validated Modified Infrastructure Survey Tool (MIST).

Conclusion

DHS is committed to using every resource available to prevent, detect, and mitigate threats of violence directed at federal facilities. Securing and protecting federal facilities is both a DHS-wide and an interagency effort.

Thank you again for the opportunity to appear before you today, and for this Committee's continued support of CISA, the Department, and our efforts. I look forward to continuing to work closely with you and other Members of Congress to keep our federal facilities, and those who work at and visit them, safe and secure.