CONVERGENCE: INTEGRATING CYBER RISK INTO FACILITY SECURITY STANDARDS

Presenter's Name
August 9, 2021

Introduction

We have young people and people starting careers who have no memory of this event. And yet they are living in a world that has been defined geopolitically, and in terms of security consciousness, by the events of 20 years ago. The next generation has grown up with the sense that terrorism is the norm, and that breaks my heart. Things will happen, and we may not always be able to prevent them. The one thing we have control over is how we respond, and that is what we at the museum call the 9/12 story. That message, that understanding that we have this capacity for compassion, resilience and hope when horrible things happen, is, I think, a tool for meeting the future.

Alice Greenwald, Chief Executive, National September 11 Memorial and Museum

Strategic Context for the CISR Mission

America's ability to adapt to a dynamic, evolving threat environment

Events of 1995 and 1996—homeland no longer secured by isolation via 2 oceans and good neighbors

PCCIP (or "Marsh Commission")—Google It!

Critical Infrastructure key to national security and economic prosperity—in a Public-Private Partnership

Call for Federal role in this space

September 11, 2001

Homeland Security Act of 2002

CISA Act of 2018

Mission Drivers

- **1993** First World Trade Center Bombing
- **1995** Oklahoma City bombing and establishment of the Interagency Security Committee
- **1996** Critical Information Assurance Office established at Department of Commerce; National Infrastructure Protection Center at FBI; Office of Energy Assurance at DOE; FedCIRC at GSA
- **1997** President's Commission on Critical Infrastructure Protection (Marsh Commission)
- **1998** Presidential Decision Directive 63 "Critical Infrastructure Protection"
- **2002** Homeland Security Act established the Infrastructure Protection function (responsibility for assessing vulnerabilities of critical infrastructure and developing a comprehensive national plan), and moved FPS and NCC (from DISA) into DHS, along with other infrastructure-focused offices
- **2003** Homeland Security Presidential Directive 7 "Critical Infrastructure Identification, Prioritization and Protection"
- **2006** National Infrastructure Protection Plan (NIPP) issued, updates in 2009 and 2013; update ongoing
- **2007** Section 550 Approps—Chemical Facility Anti-Terrorism Standards established
- **2013** Presidential Policy Directive 21 "Critical Infrastructure Security and Resilience" and E.O. 13636 "Improving Critical Infrastructure Cybersecurity" issued together

Interagency Security Committee

- On October 19, 1995, six months after the Oklahoma City bombing of the Alfred P. Murrah Federal Building, President Clinton issued Executive Order 12977, creating the Interagency Security Committee (ISC) to address continuing government-wide security for federal facilities. Prior to 1995, minimum physical security standards did not exist for nonmilitary federally owned or leased facilities.
- The Interagency Security Committee's policies, standards, and best practices are designed for Federal security professionals responsible for protecting nonmilitary federal facilities in the United States. The ISC standards and best practices help federal security professionals implement security policies and mandatory standards. The *Design-Basis Threat Report* represents the most comprehensive federal facility security standard created to date. However, this standard has been incorporated with other standards and guidance to create the Risk Management Process: An Interagency Security Committee Standard.

Convergence

- **Convergence:** A collaborative effort to enhance security through integrating operational physical security, and information assurance and technology processes, to protect federal government assets.
- Virtual/Cyber incidents cause real world impacts:
  - Financial costs
  - Physical damage
  - Information loss
  - Reputation and Indemnity
- **Necessitates**: Integrated approach to infrastructure security: First GOV integrated physical/cyber security assessment; ISC Cyber Undesirable Events 2010: CFATS RBPS-8;
- COMPLIANCE: 25 Security Benchmarks—can this be a reporting model?

Integrated Facility Security Standards

- **The Federal Information Security Management Act of 2002 (FISMA)** as amended requires each federal agency to develop, document, and implement an agency-wide program to provide information security (information assurance) for the information systems and technology (IT) that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.
- **As required by FISMA,** the National Institute for Standards and Technology (NIST) provides technical standards and guidance to executive agencies on IT security. Federal agencies must meet the minimum-security requirements using the security controls in NIST Special Publication (SP) 800-53, Security and Privacy Controls for Federal Information Systems.

Mission Centric Strategies

- **Convergence** is a comprehensive methodology for applying both the management of facilities and cybersecurity necessary for supporting and achieving various missions across federal entities. The ISC's Mission Centric Planning Model for Convergence addresses six specific areas:

For more information:
www.cisa.gov

Questions?
Sue.Armstrong@cisa.dhs.gov


CYBERSECURITY & INFRASTRUCTURE
CISA
SECURITY AGENCY