Department of Homeland Security
Cybersecurity and Infrastructure Security Agency
Directives System
Directive Number: 3540-01-0.01
Issue Date: 05/16/2023

COMPLIANCE WITH INTERAGENCY SECURITY COMMITTEE STANDARDS

I. Purpose

This Directive implements the requirements of Executive Order (EO) 12977, "Interagency Security Committee," and its associated security standards for the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA).

II. Scope of Application

This Directive applies to all CISA divisions and mission enabling offices (offices) that occupy space in federally owned or leased facilities.

III. Authorities

A. EO 12977, "Interagency Security Committee"
B. EO 14111, "Interagency Security Committee"
C. Interagency Security Committee (ISC) Standard, "The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard," 2021 Edition
D. ISC Standard, "Items Prohibited from Federal Facilities: An Interagency Security Committee Standard"
E. ISC Policy, "Planning and Response to an Active Shooter: An Interagency Security Committee Policy and Best Practices Guide," 2021 Edition
F. ISC Benchmark, "The Interagency Security Committee: Agency and Facility Compliance Benchmarks," 2019 Edition
G. DHS Policy Directive 010-01, "Active Shooter Preparedness"
H. DHS Instruction Manual 121-01-010-01, Revision 1.1, "Physical Security"

IV. Definitions

A. **Facilities Security Assessment (FSA)**: The process and final product documenting an evaluation of the security-related risks to a facility. The process analyzes potential threats, vulnerabilities and estimated consequences culminating in the risk impacting a facility using a variety of sources and information.

B. **Facility Security Committee (FSC)**: A committee that is responsible for addressing facility-specific security issues and approving the implementation of security measures and practices in a multi-tenant facility. The FSC consists of representatives of all federal

tenants in the facility, the security organization and the owning or leasing department or agency. In the case of new construction or pending lease actions, the FSC also includes the project team and the planned tenant(s).

C. **Facility Security Level (FSL)**: A risk level categorization based on the analysis of several security-related facility factors, which serves as the basis for the implementation of physical security measures specified in ISC standards.

D. **Interagency Security Committee (ISC)**: An entity established within the executive branch to: a) establish policies for security in and protection of federal facilities; b) 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 c) take such actions as may be necessary to enhance the quality and effectiveness of security and protection of federal facilities. The A/S chairs the ISC, which consists of over 100 senior level executives from 60 federal departments and agencies.

E. **Interagency Security Committee Compliance System (ISC-CS)**: A compliance-based reporting system that identifies the status of all federal agency compliance with the ISC standards.

F. **Occupant Emergency Plan (OEP)**: A written set of procedures to protect life and property in a facility under specific emergency conditions; may include procedures for evacuating the facility or sheltering in place depending on the nature of the emergency.

G. **Occupant Emergency Plan Working Group (OEPWG)**: A committee of CISA divisions and offices that coordinate emergency preparedness plans and procedures to develop the CISA OEP and its facilities where CISA is a primary occupant.

H. **Senior Risk Decision Maker**: The head of a division or office, or their designee, who makes facility risk and security planning determinations through consultation with the FSC.

V. Responsibilities

A. The **Director, CISA**:
   1. Approves CISA policies for implementation of ISC policy, standards and implementation recommendations.

B. The **Deputy Director, CISA**:
   1. Directs the appropriate and consistent application of ISC standards across CISA; and
   2. Serves as the final decision authority if conflicts arise between ISC policy and organizational resources or mission objectives.

C. The **Chief Security Officer (CSO)**:
   1. Ensures compliance with the ISC security standards within CISA;
   2. Reviews ISC-required compliance metrics reported to the ISC-CS to measure CISA compliance and to determine the needs for corrective action;
   3. Issues all supporting procedures implementing this Directive;
   4. Oversees compliance and enforcement procedures established for this Directive; and
   5. Determines the FSL for all facilities where CISA is the primary tenant.

D. The **Chief Financial Officer**:
   1. Determines the appropriate funding vehicle to address security requirements resulting from the ISC risk review and planning process for each facility; and
   2. Assists the Deputy Director and CSO in the budgeting process for all enterprise-level security requirements.

E. The **Heads of Divisions and Mission Enabling Offices**:
   1. Designate, or serve as the Senior Risk Decision Maker when so designated, to adjudicate security requirements and security procedures to meet ISC standards at the local CISA-occupied, owned or leased facility; and
   2. Ensure compliance with this Directive and supporting procedures.

F. The **Senior Risk Decision Maker**:
   1. Develops and chairs an FSC for each assigned facility to adjudicate risk decisions to meet ISC standards;[1]
   2. Develops security and associated emergency management plans and procedures; and
   3. Attends the ISC Risk Management Process and FSC annual training offered by the ISC to ensure familiarity with ISC policies and process.

VI. Requirements

A. Purpose

These compliance requirements assure implementation of ISC security requirements by each CISA division and office that occupies or owns space in federally owned or leased facilities.

B. Description

The ISC security compliance function is comprised of governance, facility security assessments, ISC risk mitigation planning, risk mitigation plan implementation and compliance and enforcement. The procedural requirements for these elements are to be further detailed in subsequently issued implementing procedural requirements for this Directive. The Senior Risk Decision Maker designated for each facility assures

1. In cases where an existing FSC is in place at the facility, the Senior Risk Decision Maker is to participate in the FSC to address CISA space equities.

implementation of these requirements through a biannual FSC meeting forum comprised of all federal tenants of that facility.

1. **Governance**
   a. The FSC conducts security planning and makes decisions on risk mitigation for each owned or leased federal facility in which CISA is an occupant, including in single and federal tenant facilities and produces deliverables as required by ISC standards.
   b. The Senior Risk Decision Maker convenes meetings to develop or revise, when needed, a security risk mitigation plan for the facility, primarily based on an approved facility security assessment led by the Office of the Chief Security Officer (OCSO).
   c. Additional meetings may be required to address or review emerging threat information, develop mitigation strategies or disseminate security alerts.

2. **FSA**
   a. The FSA is scheduled by the OCSO for each facility in accordance with prescribed intervals identified in ISC's "The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard," which can be accessed on the CISA publications website.
      i. The CSO schedules FSAs and evaluates security requirements and compliance standards to meet ISC security standards.
      ii. The FSA identifies building-specific information to develop the initial FSL and is comprised of the following elements: a signed FSL by the Senior Risk Decision Maker, security evaluations and recommendations for the FSL of the facility and the approval of the identified risk recommendations by the Senior Risk Decision Maker.

3. **ISC Facility Risk Mitigation Planning**
   a. Each facility is required to implement the following ISC risk management compliance elements in an overall plan, as detailed in "The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard," as found on the CISA publications website.
      i. Active Shooter Requirements: An active shooter preparedness plan that is to be updated at least every two years, or as needed. Either the FSC or other agency representatives are required to collaborate with other tenants or agencies to develop the plan.
         1) The Senior Risk Decision Maker is accountable for developing the plan, maintaining, storing and making it available to other tenants.
      ii. OEPs: An OEP describes the actions occupants should take to ensure their safety in a security incident-based emergency.
      iii. Mail Security Plan: A Mail Security Plan details the screening, sorting and delivery of mail and coordinates procedures for suspicious mail and incident responses.
      iv. Prohibited Items Standards: Each facility is required to assure adherence to the ISC Prohibited Items Standards that bar any item prohibited by applicable

federal, state or local law as well as prohibit items such as firearms, projectiles, chemicals and other dangerous weapons from entering the facility.

4. **Risk Management Plan Implementation**
   a. Training Requirements
      i. The FSC, in conjunction with the OEPWG, provides training, materials or awareness discussions to inform employees and contractors of security preparedness and ISC security requirements.
   b. Budgeting for Enterprise-Level Facility Security Requirements
      i. The FSC determines whether to implement a security countermeasure or document risk acceptance. The Senior Risk Decision Maker documents these decisions and coordinates with the Office of the Chief Financial Officer to fund individual countermeasures using the appropriate budget and funding vehicle.
      ii. When security countermeasures apply to all CISA facilities or there is an economy-of-scale in addressing countermeasures collectively, OCSO documents the requirement as part of the CISA budgeting process.

VII. Compliance and Enforcement

A. Consequences for Noncompliance: Noncompliance with ISC standards may leave CISA exposed to risks in protecting its workforce and federal facilities.

B. Compliance Procedures: OCSO maintains the repository of FSA reports and decisions documented by Senior Risk Decision Makers and provides an annual summary to the CISA Director and the heads of divisions and offices upon request. OCSO identifies the status of ISC compliance within CISA and provides recommendations to the Director to ensure compliance with ISC standards.

C. Enforcement Methods: OCSO conducts an annual review of CISA's compliance with the ISC Risk Management Process using the ISC compliance benchmarks and enters its compliance report into the ISC-CS database and the CISA Enterprise Risk Management System.

D. All CISA divisions and offices are required to comply with this Directive, any associated procedures and all related federal policies and standards. The CSO is responsible for overseeing the compliance and enforcement of this Directive.

VIII. Questions

Address any questions or concerns regarding this Directive to OCSO, (b) (6)

Summary of Changes:

Section Reference	Type of Change	Concise Description	Author/Approving Authority (Name, Office/Division)	Date
Section III. "Authorities"	*Administrative*	*Added EO 14111 to "Authorities"*	*Joe Cassone, OCSO* *Meghan Chiles, SPP*	*4/28/2025* *5/1/2025*

(b) (6)

Jen Easterly, Director
Cybersecurity and Infrastructure Security Agency

05/16/2023
Date