Interagency Security Committee

2018 Annual Report

CISA
CYBER+INFRASTRUCTURE

Message from the Chair

I am pleased to present the *Interagency Security Committee 2018 Annual Report*. Established in 1995 by Executive Order 12977 in response to the bombing of the Alfred P. Murrah Federal Building in Oklahoma City, the Interagency Security Committee (ISC) has sought to assist Federal Departments and Agencies to make defensible, risk-based, and resource-informed security decisions with the objective of enhancing the security posture of Federal facilities across the nation.

This report highlights many of the ISC's accomplishments and activities in 2018, including the continued development of the ISC Compliance System database for Departments and Agencies to report their level of compliance with ISC policies and standards. This operational system represents a major step in fulfilling the ISC's requirement to ensure compliance. The ISC also supported the completion of over 5,600 online and in-person courses on the ISC's Risk Management Process and Facility Security Committees' duties and responsibilities.

Lastly, this report captures the hard work and collaboration that occurs across the ISC. The ISC works by, with, and through its members, and the successes outlined in this report are the result of the exemplary effort put forth by members who volunteer their time to create, update, and implement ISC policies, standards, and recommendations. I thank them for their continued dedication to the important mission of securing Federal facilities.

Brian Harrell
Assistant Director for Infrastructure Security
Cybersecurity and Infrastructure Security Agency

Table of Contents:

The Interagency Security Committee 2018 Annual Report

Oklahoma City Federal Building

Established by Executive Order 12977, the mission of the ISC, through its member Departments and Agencies, is to enhance the quality and effectiveness of security in, and protection of, facilities in the United States occupied by Federal employees for nonmilitary activities. The ISC is a permanent interagency body that addresses continuing government-wide security concerns.

This Annual Report provides stakeholders with a snapshot of the Committee's activities and accomplishments over the course of 2018, and also highlights future plans and initiatives expected in 2019. Identifying the ISC's annual progress and measuring the performance of its various security initiatives is an important feedback mechanism. This report is organized by major ISC lines of effort: Compliance, Updated Publications, Training, and Outreach.

Compliance

Executive Order 12977 requires the ISC to "develop a strategy for ensuring compliance." The creation of the ISC's Compliance Program is a major step towards fulfilling that requirement. There are five components that make up the ISC's Compliance Program.

Compliance Program:

Compliance Subcommittee: Develops strategy for ensuring compliance with established standards

Compliance Memo: Defines the vision and expectations of the ISC Compliance Program

Benchmarks and Instructional Guide: Establishes baseline requirements to assess compliance with ISC standards

National Compliance Advisory Initiative: Conducts outreach focused on relationship building, engagement, and education

ISC Compliance System: Houses facility data and serves as a tool to monitor compliance

Major Milestone: Limited Rollout of the ISC Compliance System (ISC-CS)

In the summer of 2018, the ISC executed a limited rollout of its Compliance System (ISC-CS) to 11 Departments and Agencies. The ISC-CS is a centralized and secure database designed to provide analytical capability and insight into a Department or Agency's compliance with ISC policies and standards. The Departments and Agencies that participated in the limited rollout dedicated their time and resources to testing the new system by inputting some or all of their facility compliance data.

Following the conclusion of the limited rollout, the ISC collected feedback from participants and, based on this feedback, is currently working to improve the system's interface, accessibility, and overall user experience in order to make the system as user-friendly as possible. The ISC is also refining its ISC-CS supporting efforts to solidify best practices, identify keys to success, and ensure better system usability for the full rollout slated for 2019. In addition to the improvements being made within the database, the results of the limited rollout aided in updating the compliance benchmarks, the means by which the ISC measures Department and Agency compliance with policies and standards. The new benchmarks, which are expected to be published in early 2019, will reduce ambiguity and create more consistent data reporting.

The limited rollout marks a significant maturation in the ISC's Compliance Program. The ISC will not only publish security guidance, but it will, for the first time, begin to monitor compliance with its policies and standards, thus placing the ISC in a position to provide compliance assistance to Departments and Agencies that are most in need.

U.S. DEPARTMENT OF HOMELAND SECURITY
S&T
USCG
USSS
USCIS
CBP
TSA
IRS
EEOC
NARA
ODNI

The 11 Departments and Agencies that participated in the ISC-CS limited rollout

Updated Publications

One of the responsibilities of the ISC is to develop policies, standards, and recommendations through interagency Subcommittees and Working Groups. One of these standards is the *Risk Management Process for Federal Facilities: An Interagency Security Committee Standard* (RMP). In 2018, the ISC updated two of the six appendices of the RMP:

RMP Appendix A:
Design-Basis Threat Report (FOUO)

RMP Appendix B:
Countermeasures (FOUO)

The Design-Basis Threat Subcommittee added one Undesirable Event: Adversarial Use of Unmanned Aircraft Systems. The Countermeasures Subcommittee added a comprehensive reference to policies meant to increase compliance with Homeland Security Presidential Directive (HSPD-12), and Vehicle Ramming mitigation measures.

In addition to the revisions made to the RMP Appendices, ISC Working Group members made significant progress in updating other ISC publications, including *Violence in the Federal Workplace: A Guide to Prevention and Response*. The ISC's active Working Groups include:

- Workplace Violence
- Construction Standards
- Armed Contract Security Officers
- Protection Center for Excellence

ISC Certifies Two Members' Risk Assessment Tools

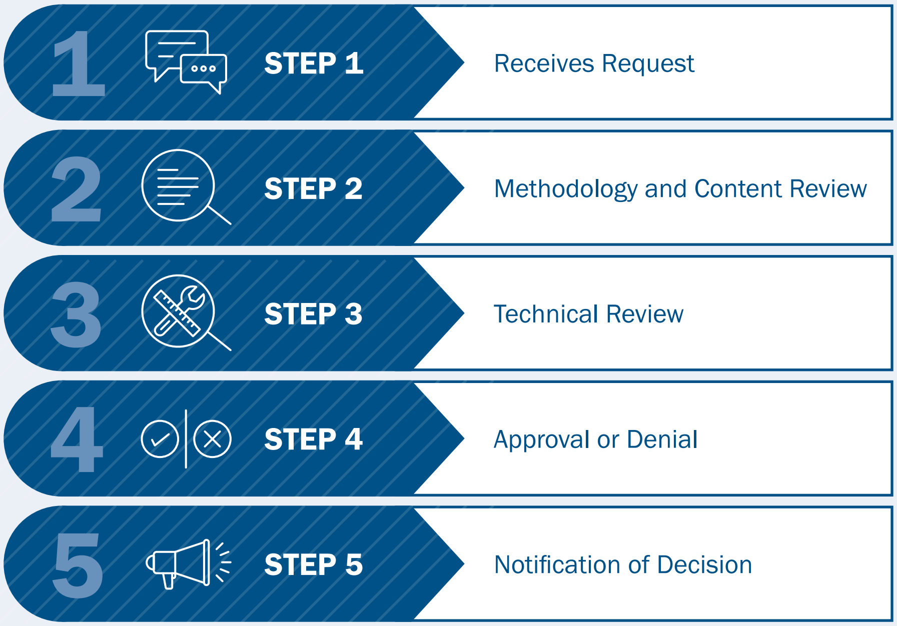
This year, the ISC validated two new risk management tools: the Federal Protective Service (FPS) Modified Infrastructure Survey Tool (MIST) 2.0 and the U.S. Customs and Border Protection (CBP) SMART (CM) tool. The validation of these two tools brings the total number of ISC-validated tools for use by Federal Departments and Agencies to eight.

MIST 2.0 is a protective tool suite that captures, stores, and accesses information associated with the protection of federal facilities. This information supports the creation of Facility Security Assessments (FSAs) to guide risk management recommendations for the protection of those facilities.

CBP's SMART tool can calculate a building's Facility Security Level (FSL), account for the threats identified in Appendix A, and allow for the customization of countermeasures in Appendix B to ensure they meet the unique security needs of specific facilities.

The ISC's Tool Validation Board, composed of member representatives, works with member Departments and Agencies to assess and validate risk assessment tools against ISC standards. The tool validation process involves five steps: (1) ISC receives request; (2) methodology and content review; (3) technical review; (4) approval or denial; and (5) notification of decision.

ISC Risk Management Tool Validation Workflow Process



1 STEP 1 Receives Request

2 STEP 2 Methodology and Content Review

3 STEP 3 Technical Review

4 STEP 4 Approval or Denial

5 STEP 5 Notification of Decision

The procedure listed above outlines the approval process for requesting the validation of a risk assessment tool.

Training

National Compliance Advisory Initiative

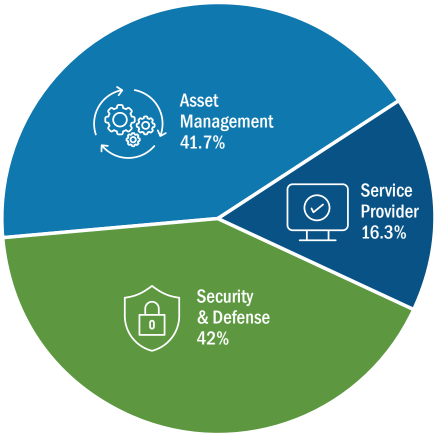
The National Compliance Advisory Initiative (NCAI) is an effort aimed at supporting Departments and Agencies seeking to achieve compliance with ISC policies, standards, and recommendations. NCAI Phase 2 consists of a half-day course which covers the Risk Management Process Standard and the roles and responsibilities of Facility Security Committees. In 2018, the ISC held 29 engagements and trained over 800 students. In 2020 and beyond, the NCAI will include the provision of direct assistance to Departments and Agencies and, ultimately, the verification of compliance with ISC policies and standards.

2018 NCAI Metrics

876	Participants
92%	Average Exam Score
51	Participating Departments, Agencies, and Organizations*
93%	Positive Composite Feedback Score

* Organizations refer to state, local, or private sector entities.

NCAI 2018 Participants by Mission Area



143 (16.3%) trainees represent Departments, Agencies, or Organizations whose mission is to provide a service to the U.S. public.	The Department of Veterans Affairs (VA), the Social Security Administration (SSA), and the U.S. Department of Agriculture (USDA).**
365 (41.7%) trainees represent Departments, Agencies, or Organizations that manage and oversee resources.	General Services Administration (GSA), Office of Personnel Management (OPM), and Internal Revenue Service (IRS).**
369 (42%) trainees represent Departments, Agencies, or Organizations that secure or defend U.S. infrastructure, information, or people.	Federal Protective Service (FPS), the Department of Homeland Security (DHS HQ), and the Department of Defense (DOD).**

** Agencies listed above represent a sampling of participating agencies

RMP Training Wins Award

This year, the first course and tool certified by the ISC received the Gold American Security Today "ASTORS" Award for Best Federal Government Security Training Program. *American Security Today* awarded the Federal Risk Management Process Training Program (Fed RMPTP) with this award for providing a comprehensive, hands-on training led by industry experts. The 3-day course teaches students how to develop a Facility Security Level, identify Baseline Levels of Protection, identify and assess risks, determine necessary or highest achievable Level of Protection, and implement countermeasures utilizing the ISC Risk Management Process.

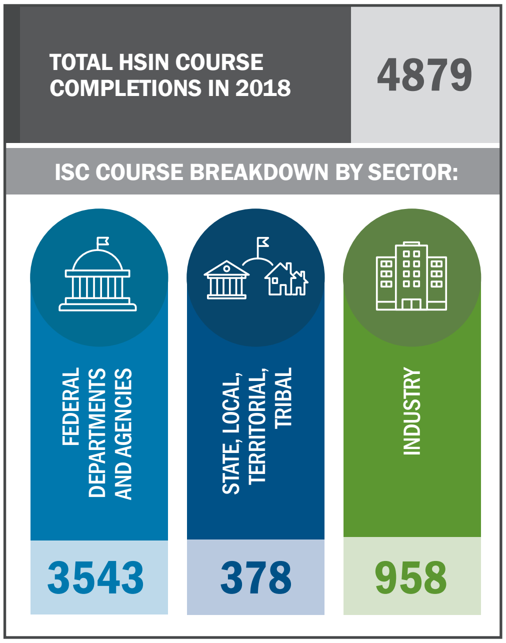
Pictured left to right: John Rossiter, Securities and Exchange Commission; Michael Madsen, American Security Today; Reid Hilliard, Department of Justice; and Kevin McCombs, Office of Personnel Management

Training

Online Training:

The Homeland Security Information Network (HSIN) provides users with online versions of the ISC's in-person National Compliance Advisory Initiative (NCAI) training modules. The ISC developed these online training courses to provide Federal security professionals, engineers, building owners, architects, and the general public with information pertaining to the ISC and its security polices, standards, and recommendations. The training course is comprised of five lessons:

- Introduction to the ISC
- Overview of ISC Publications
- Risk Management Process for Federal Facilities: Facility Security Level (FSL) Determination
- (FOUO) Levels of Protection (LOP) and Application of the Design-Basis Threat Report
- Facility Security Committees (FSC)



TOTAL HSIN COURSE COMPLETIONS IN 2018: 4879

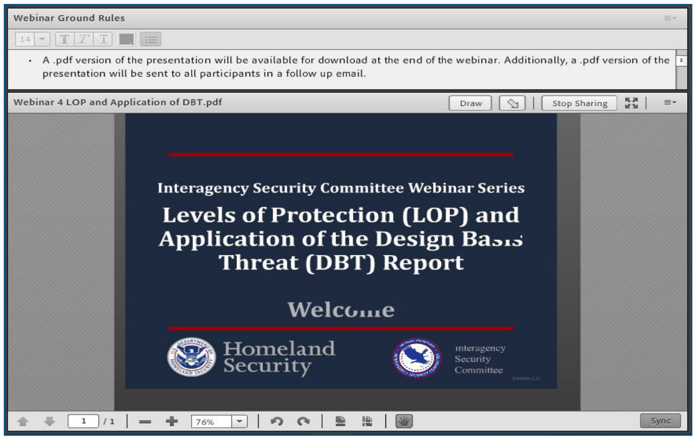
ISC COURSE BREAKDOWN BY SECTOR:

FEDERAL DEPARTMENTS AND AGENCIES	STATE, LOCAL, TERRITORIAL, TRIBAL	INDUSTRY
3543	378	958

Webinars:

Each year, the ISC hosts webinars to educate stakeholders on ISC policies, standards, and recommendations. In 2018, the ISC held two webinars titled *Determining Facility Security Levels and Baseline Levels of Protection* and *Levels of Protection and the Application of the Design-Basis Threat Report*.

279*	Total Webinar Participants in 2018 **161 individuals attended webinar 1 and 118 attended webinar 2*
100%	Participants who "Agree" or "Strongly Agree" that ISC webinars made them more aware of resources to help increase their organization's security preparedness
99.3%	Average percentage of webinar participants who believe they will utilize the information they learn during ISC webinars.



Webinar Ground Rules

- A .pdf version of the presentation will be available for download at the end of the webinar. Additionally, a .pdf version of the presentation will be sent to all participants in a follow up email.

Webinar 4 LOP and Application of DBT.pdf

Interagency Security Committee Webinar Series

Levels of Protection (LOP) and Application of the Design Basis Threat (DBT) Report

Welcome

The ISC hosts webinars on Homeland Security Information Network (HSIN) Connect.

Outreach

Bilateral Engagements:

In 2018, ISC leadership held bilateral meetings with 41 of its members. These meetings, which are held on an annual basis, provide an opportunity for members to discuss their unique perspectives on the facility security issues impacting their Department or Agency.

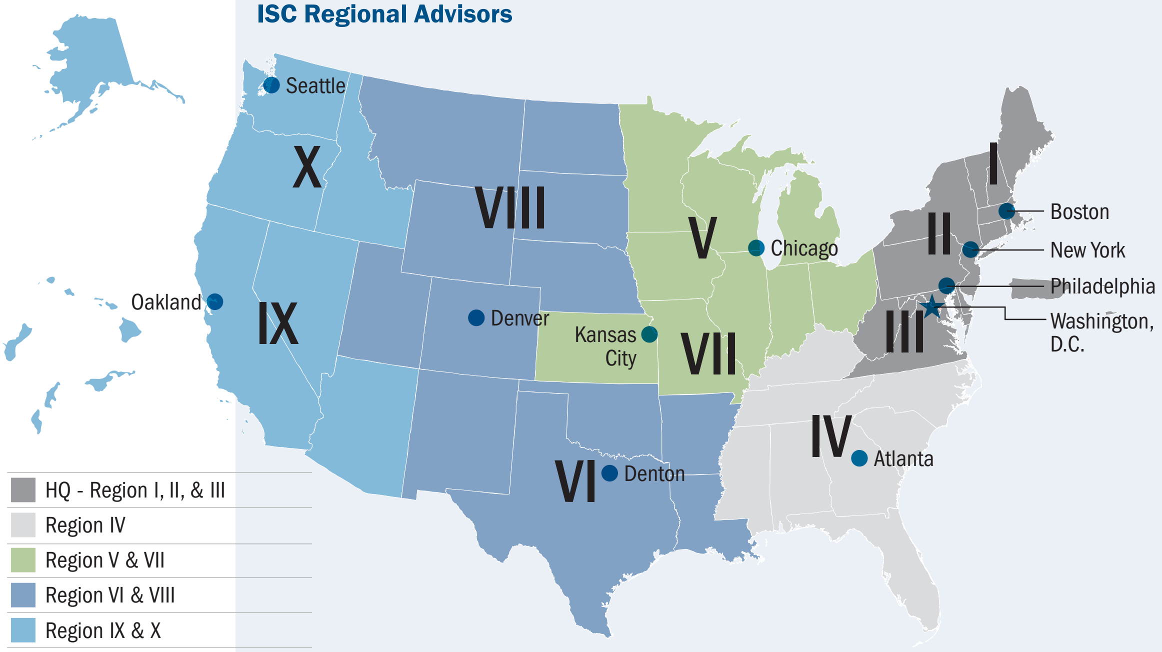
New Regional Advisors Support Outreach Efforts

In 2018, the ISC extended its reach across the nation by onboarding four Regional Advisors. For the first time ever, the ISC has staff available to connect directly with the ISC stakeholders in their regions.

The majority of the Regional Advisor efforts focus on informing regional stakeholders about ISC policies, standards, and recommendations and the importance of reaching Federal facility security compliance. Regional Advisors assist stakeholders in a variety of ways, including visits and consultations with Facility Security Committees and Federal Executive Boards, answering compliance and facility-specific questions, and serving as a resource for all ISC-related questions and concerns.

Regional Advisors provide unique support to regional stakeholders in that they are familiar with their regions and are readily accessible to the individuals they serve. They also connect with non-member Federal, state, and local entities that may not be familiar with the ISC and its policies, standards, or recommendations. This helps support the ISC's larger effort of informing non-member Executive Departments and Agencies of their requirement to be compliant with ISC policies and standards.

ISC Regional Advisors



*Cities listed on map represent regional office locations

The Way Forward:

Federal Aviation Administration

2019 Working Groups:

In 2019, the ISC will form at least two new Working Groups to address issues of national significance that are increasingly impacting the Federal facility security community: threats from unmanned aerial systems (UAS) and challenges related to physical access control.

The mission of the *Protecting Against the Threat of UAS Working Group* will be to develop best practices and lessons learned to assist Departments and Agencies with establishing programs and countermeasures to address the emerging risk posed by UAS. While the ISC's Countermeasures document provides general guidance applicable to the UAS threat, the nature, proliferation, and potential threat of UAS requires additional attention. The Working Group will publish best practices for Departments and Agencies and identify opportunities to save time and resources.

The primary mission of the *Physical Access Control Working Group* will be to examine the issue holistically, identify best practices and lessons learned, and inform agencies on how best to implement physical access control systems that comply with various Federal policies.

St. Elizabeths Campus, Department of Homeland Security

ISC: The Way Forward:

2018 was a significant year for the ISC. The ISC began executing the rollout of the ISC-CS, increased its member outreach efforts by establishing Regional Advisors, and trained a record number of individuals.

The ISC looks forward to continuing these and other important initiatives in 2019, including the full rollout of the Compliance System to additional member Departments and Agencies. Together, members of the ISC are working to increase the safety and security of Federal facilities across the nation.

Front Cover: Jacob K. Javits Federal Building, New York, NY
Back Cover: Frank M. Johnson Federal Building and U.S. Courthouse, Montgomery, AL

For general inquiries, including questions for ISC Staff and Regional Advisors, please contact:
ISC@hq.dhs.gov

For access to ISC Publications, please contact:
ISCAccess@hq.dhs.gov

For questions related to the rollout of the Compliance System, please contact:
ISCCS-Support@hq.dhs.gov