Interagency Security Committee

2022 Annual Review

MARCH 2023

U.S. Department of Homeland Security
Cybersecurity and Infrastructure Security Agency

Message from the Chair

Greetings to our partners in federal facility security. This year presented an array of new challenges, obstacles, and threats to federal facilities, but as public servants, each member has accepted the challenge presented and risen to the occasion of protecting the homeland. The Interagency Security Committee (ISC) continues to be an integral component in national security, protecting federal facilities, and enhancing overall resilience. The ISC has brought together 66 federal departments and agencies to address and combat potential threats to federal facilities and personnel.

As the threats to our federal facilities remain heightened, much as they have been the last few years, and domestic violent extremists persist in targeting our government, the need for pertinent policies and best practices is ever-present. The ISC, therefore, must dedicate itself more than ever to producing relevant policy and standard guidance and taking leadership in establishing best practices, as it has done successfully in previous years through the work of its dedicated membership. Most recently, these successes include the development of all publications through ISC subcommittees and working groups and the 2022 release of publications such as the Security Specialist Career Progression Ladder: An Interagency Security Committee Guide, 2022 Edition.

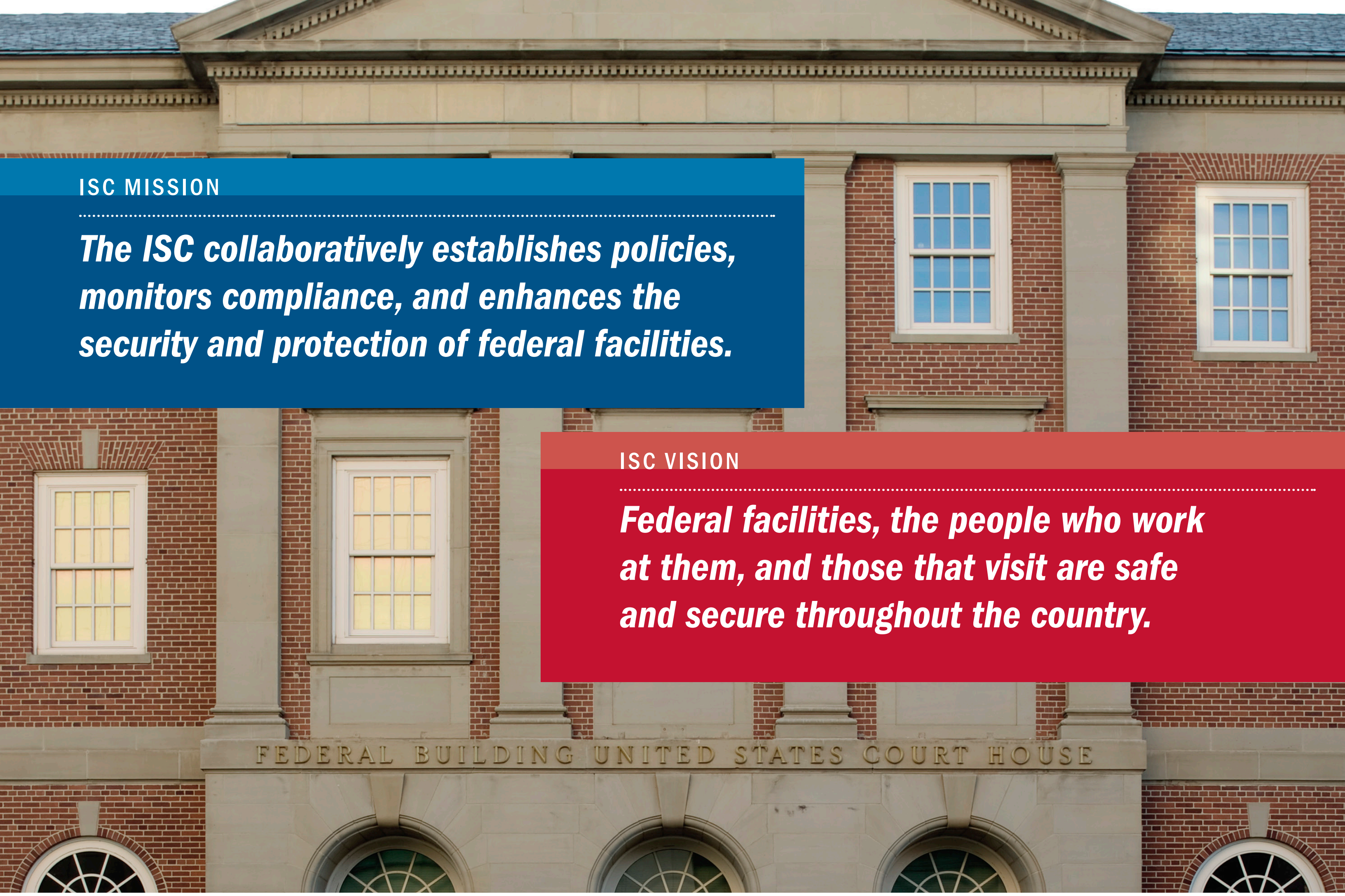
In Fall 2022, the enactment of *Title 41, Part 102-81: Federal Management Regulation (FMR); Physical Security* went into effect. *Title 41 Part 102-81* states that each agency and federal facility operating under the jurisdiction, custody, or control of the General Services Administration (GSA) must comply with the policies and recommendations set forth by the ISC, including The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard (RMP Standard). This rule, in addition to the critical updates being made to Executive Order (EO) 12977, demonstrates the importance our national leadership places on the protection of federal facilities nationwide.

Compliance continues to prove an invaluable tool with the successful completion of the Compliance Verification Pilot program. This year's compliance reporting continued to grow, to include 100 percent of our non-exempt members reporting. Well done.

Once again, the 2022 Annual Review includes a collection of entries from ISC members which highlight the impactful work being conducted by departments and agencies in the field, entitled ***Profiles in Excellence***. These pieces are associated with several areas of importance in which the ISC is excelling: expertise and guidance, capacity building, assessments and analysis, and security operations. These entries are a testament to the enduring strength and importance of the ISC.

Finally, I would like to thank and congratulate all 66 members of the ISC for another year of offering invaluable expertise, leadership, and dedication to the mission of the ISC. Your commitment to advancing the mission of the ISC and to protecting all federal facilities and those who work, and visit, these facilities is unparalleled and deeply appreciated.

David Mussington, PhD
Executive Assistant Director for Infrastructure Security
Cybersecurity and Infrastructure Security Agency



ISC MISSION

The ISC collaboratively establishes policies, monitors compliance, and enhances the security and protection of federal facilities.

ISC VISION

Federal facilities, the people who work at them, and those that visit are safe and secure throughout the country.

Table of Contents

Executive Summary

The Interagency Security Committee (ISC) 2022 Annual Review highlights the ISC's continued dedication to providing its 66 members with excellence in federal security guidance, best practices, and training opportunities. As highlighted within this Review, in 2022 the ISC successfully completed another year of compliance reporting with 100 percent of facilities having reported, published updated appendices to The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard (RMP Standard) along with several other publications, offered both in-person and virtual Risk Management Process (RMP) and Facility Security Committee (FSC) training, and hosted 56 annual meetings with ISC members.

The 2022 Annual Review includes substantial feats from the following categories: **Strengthening ISC Authorities**; **Compliance**; **Policies, Standards, and Recommendations**; **Training**; **Regional Advisors**; and **Outreach**. In addition, the pertinent work of several ISC members and the policies and programs they have enacted to ensure enhanced security at federal facilities are highlighted throughout this Review.

Below: The Joel Solomon Federal Building and U.S. Courthouse, Chattanooga, TN
Previous: Ewing T. Kerr Federal Building, Casper, WY

Credit: U.S. General Services Administration Historic Building Photographs

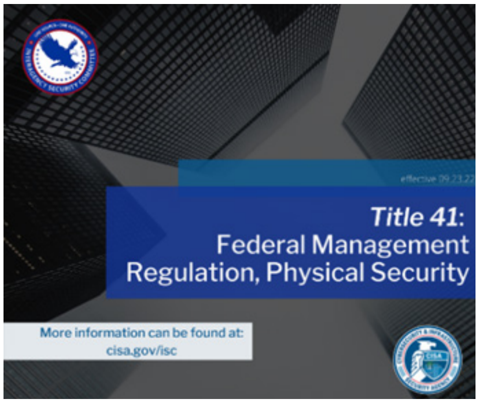
Strengthening ISC Authorities

In 2022, the ISC's authorities for setting, implementing, and monitoring security policies and standards were reinforced through the publication of *Title 41, Part 102-81: Federal Management Regulation (FMR); Physical Security*, as well as the ongoing effort to refresh Executive Order (EO) 12977.

Title 41: Part 102-81, Physical Security

In Fall 2022, the General Services Administration (GSA) amended *Title 41 Part 102-81* to clarify the responsibilities of agencies in maintaining physical security standards in and at federally owned and leased facilities and grounds under the jurisdiction, custody, or control of GSA. *Title 41 Part 102-81* reinforces the ISC's existing EO authorities by codifying them in the FMR.

The ISC issued the initial RMP Standard in August 2013 to define the criteria and processes to determine the Facility Security Level (FSL) and provide a single source of physical security countermeasures for nonmilitary federal facilities. *Title 41 Part 102-81* clarifies, under EO 12977, that the ISC is responsible for setting policies and recommendations to govern physical security at nonmilitary federal facilities and buildings under the jurisdiction, custody, or control of GSA. It also confirms that each of these GSA facilities must comply with the policies and recommendations set forth by the ISC, including the RMP Standard.



effective 09.23.22

Title 41:
Federal Management
Regulation, Physical Security

More information can be found at:
cisa.gov/isc

Key changes to Title 41 Part 102-81 made in 2022 include the following points:

- ISC's RMP Standard is the benchmark to determine FSL.
- ISC policies and recommendations have been established as governing physical security.
- Agencies occupying GSA space are identified as being responsible for implementing, maintaining, and upgrading physical security standards.
- Federal occupants will be responsible for funding a *pro-rata* share of the cost once countermeasures are approved.
- GSA will coordinate for physical security clauses when acquiring leased facilities or managing new construction.

Update to EO 12977

Photograph by Chip Somodevilla / Getty

To address ongoing and emerging threats, National Security Council (NSC) staff, through the Homeland and Critical Infrastructure Resilience Interagency Policy Committee (HCIR IPC), initiated a process to evaluate and revise EO 12977 in 2021. In 2022, the HCIR IPC and NSC legal team completed the EO review and moved it to the Deputies Committee for approval. The Sub-IPC members' inputs will ensure the ISC is postured to address the shifting threat environment in federal facility security for at least another 27 years. The new EO is expected to be signed by the President in Spring 2023.

Changes and impacts of the new EO include:

- Updates to duties and responsibilities to better reflect the limits of the ISC's authority and responsibility
- Requirements to provide best practices for mobile federal workforce security
- Obligation to submit a biennial report detailing compliance results to the Director of the Office of Management and Budget and the Assistant to the President for National Security Affairs
- Mandate for each department and agency to designate a senior official responsible for implementation and compliance with the EO, and to support facility security committees
- Establishment of minimum compliance monitoring requirements for the Department of Homeland Security (DHS) to include when conducting risk-based compliance verification
- Clarification of the definition of federal facilities to reduce ambiguity

PROFILES IN EXCELLENCE

DHS's Office of the Chief Security Officer (OCSO)

Through ISC support, outreach, and education efforts, ***DHS's Office of the Chief Security Officer*** led an enterprise-wide effort to increase physical security awareness and ensure compliance with ISC standards. Led by OCSO's Strategic Operations Division (StratOps), OCSO became a key contributor in ISC policy development. This effort also ensured any updated policies were captured in DHS security standards and incorporated into OCSO Security Performance Audits.

StratOps provided oversight and component coordination in ISC initiatives. The Division also served as the primary point of contact for and liaison with the Federal Protective Service (FPS) to oversee and manage DHS facility physical security data.

As part of this effort, StratOps coordinated and conducted Facility Security Assessment (FSA) training, using the FPS Modified Infrastructure Survey Tool, and ensured that ISC-Compliance System (ISC-CS) benchmark reporting requirements remained on track. For their efforts, StratOps received special recognition from the Chief of the ISC, namely for assisting in the development and refinement of facility security compliance verification procedures and achieving the best Agency Composite Engagement Score (ACES) in the large agency category.

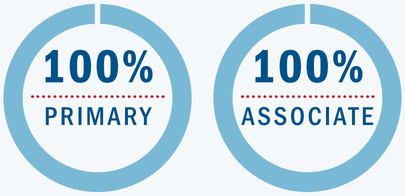
Compliance

ISC members successfully completed the fourth year of compliance reporting while increasing the level of reporting among all members and enhancing levels of compliance across the Committee. Compliance reporting provides ISC members with the means to measure, report, and analyze compliance with the ISC policies and standards. This year was a major undertaking by all to achieve the Compliance Subcommittee's goal of reporting on 100 percent of organization benchmarks and 100 percent of facility portfolios.

The compliance reporting initiative had immense support from ISC membership, with 53 members and all non-exempt members reporting in 2022. Additionally, nine members, who are not required to report due to EO exemptions or being outside of the Executive Branch, found value in reporting, and one new member reported for the first time.

There were 218 sub-organization benchmarks and 14,100 facility benchmarks completed and certified in 2022. The average organization compliance score increased from 4.0 out of 5.0 last year to 4.1 this year while the average facility score increased from 3.5 last year to 3.6 this year. Additionally, during the 2022 reporting period, the compliance staff responded to over 317 compliance assistance requests.

Percentage of ISC Members Reported*



*Excludes Exempt Members

Total Numbers Reported

218 Org. Benchmarks Submitted

14,100 Facility Benchmarks Submitted

Net gain of 3 sub-orgs and nearly 3,000 additional facilities from FY 2021

Average Compliance Scores

Org. Score	4.0 ↗	**4.1**
Facility Score	3.5 ↗	**3.6**

Org. compliance score increased from 4.0 and Facility score from 3.5 in FY 2022

Compliance Verification Pilot Program and Full Implementation

In 2022, the ISC established a Compliance Verification program to provide an independent, third-party verification of compliance at the organizational, sub-organizational, and facility levels. Compliance Verification involves analyzing a department's or agency's reported compliance data and providing recommendations on ways to improve compliance.

The 2022 Compliance Verification Pilot enabled a smooth rollout of Compliance Verification and helped refine processes and procedures while also gathering requirements for staffing, responsibilities, and training. The Verification Pilot was implemented in an incremental approach using five pilot verifications. ***Thank you*** to the National Archives and Records Administration, Internal Revenue Service (IRS), Department of Commerce (DOC), DHS, and Environmental

Protection Agency (EPA) for volunteering as host organizations for this program, and to the verification team members who volunteered to assist with verification reviews alongside the ISC staff.

Benefits of Compliance Verification

- Verify reporting accuracy
- Enhance communication
- Analyze ISC policy implementation
- Observe and share best practices between organizations

Verification Pilot reviews involved the analysis of nine organization-level benchmarks from Fiscal Year (FY) 2021, which is the most recent set of certified scores. These benchmarks cover an organization's implementation of ISC policies and standards, utilization of the RMP Standard, risk acceptance documentation, and guidance and support to FSCs. The host organizations were provided a verification checklist in advance of the program and submitted documentation to support their reported benchmark scores. During the pilot, the compliance team uncovered several lessons learned and used them to better build out the program going forward.

Now that the Verification Pilot is complete, the ISC will begin to conduct Compliance Verification Reviews throughout 2023, with organizations being selected using risk-based selection criteria and approved by the Compliance Subcommittee to ensure the approach is credible, reproducible, and defensible. The risk-based approach for verification selection considers vulnerability, consequence, and threat, utilizing an organization's annual compliance reporting inputs. With a risk-based approach, the Compliance Subcommittee can ensure all efforts are appropriate to the risk environment and are focused on where they can produce the most effective outcomes.

Compliance Verification Reviews culminate with a formal report and out-brief to the organization that contains observations, recommendations, and best practices. Full implementation of Compliance Verification is set to begin in Quarter 2 of FY 2023. For additional information or questions contact ISC-Verification@cisa.dhs.gov.

PROFILES IN EXCELLENCE

Federal Emergency Management Agency (FEMA) Creates Innovative Solutions

Since 2009, ***FEMA's OCSO, Field Security Division (FSD), Physical Security Branch (PSB), Asset Protection Management Section (APMS)*** has conducted facility risk assessments for temporary facilities owned, leased, or occupied by federal employees. During the 2017 disaster season, FSD leadership realized the need to augment the Reservist Security Core process and added site selection, FSL determinations, and facility risk assessments. The number of assessments, coupled with limited staff, led the APMS team to innovate and implement virtual facility risk assessments. With the help of the security reservist on site, APMS team members were able to conduct assessments via phone or video calls, utilizing the video and pictures as visual tools for completion.

FSD's three branches—PSB, Security Technology Integrations and Analytics Branch (STIAB), and Disaster Security Branch—have saved the government millions of dollars on the management of disaster sites. Through their creative collaboration, these branches have installed countermeasures to reduce risk, reduced the need for a 24/7 security guard, and raised the overall security posture of disaster sites. By conducting an assessment, identifying the need for an Intrusion Detection System (IDS) as a minimum, coordinating the efforts with STIAB and the security reservist on site, the guard hours can be cut in half, relying on the IDS to secure the facility when it is closed in the evenings.

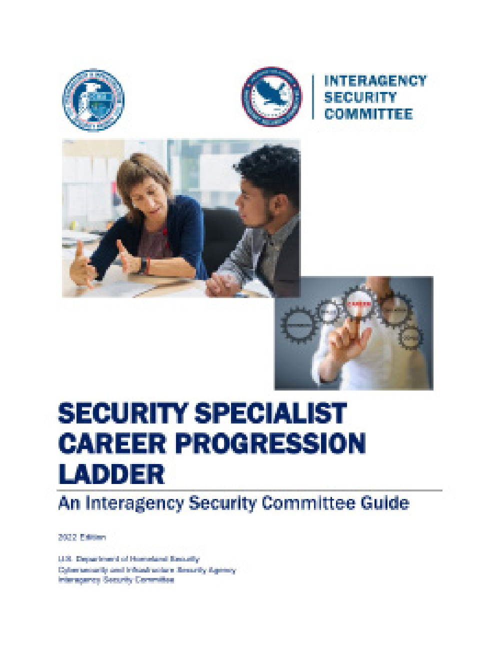
In 2022, the APMS team collaborated with all stakeholders and educated senior leaders on the ISC standards and benefits of using the tool FEMA developed. In 2022, the APMS team has conducted over 50 disaster security facility assessments.

Policies, Standards, and Recommendations

The ISC's Policies, Standards, and Recommendations directly support the ISC mission to "collaboratively establish policies, monitor compliance, and enhance the security and protection of federal facilities." Presently, the ISC maintains a library of over 20 documents which include standards, policies, best practices, white papers, templates, and guides.

These resources lay the foundation for the work of the ISC and serve as a collaborative roadmap to protect federal facilities and those who work at and visit them. ISC policies and standards are scalable and tailorable resources to identify and address site-specific federal facility security needs. ISC policies and standards assist with the creation and implementation of initiatives to enhance security beyond the baseline requirements.

2022 PUBLICATIONS



INTERAGENCY SECURITY COMMITTEE

SECURITY SPECIALIST CAREER PROGRESSION LADDER

An Interagency Security Committee Guide

2022 Edition

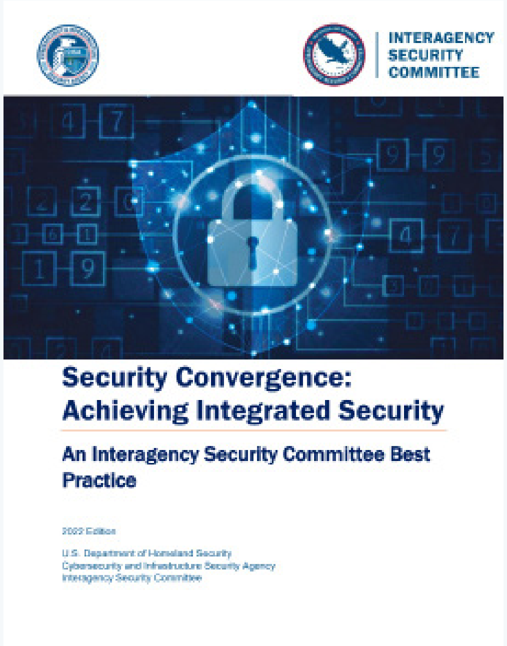
U.S. Department of Homeland Security
Cybersecurity and Infrastructure Security Agency
Interagency Security Committee

Security Specialist Career Progression Ladder, An Interagency Security Committee Guide, 2022 Edition

This 2022 edition is intended to be a companion to the *Security Specialist Competencies: An Interagency Security Committee Guide*. It provides a methodology along with resources on how to advance security specialist knowledge and skills, identify existing knowledge gaps, and grow as well-rounded security professionals. The guide also assists supervisors and employees in discussions on professional development.

Key areas in this document include:

- Identifying goals, pinpointing areas for growth, and creating a plan for success
- Understanding security specialist core, supervisory, and technical competencies
- Discovering training and professional development opportunities to build skills and maximize potential



INTERAGENCY SECURITY COMMITTEE

Security Convergence: Achieving Integrated Security

An Interagency Security Committee Best Practice

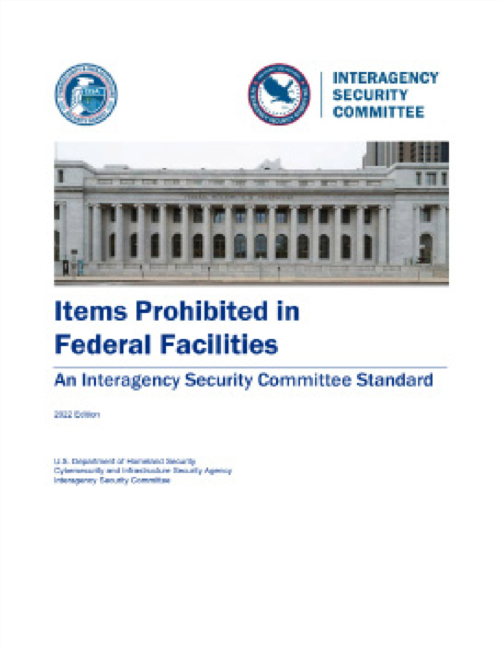
2022 Edition

U.S. Department of Homeland Security
Cybersecurity and Infrastructure Security Agency
Interagency Security Committee

Security Convergence: Achieving Integrated Security, An Interagency Security Committee Best Practice, 2022 Edition

This best practice guide assists organizations seeking to achieve integrated security through a collaborative effort between physical security, information security, cybersecurity, information assurance, and information technology to protect their assets.

It provides guidance to assist federal executive branch departments and agencies in achieving integrated security through best practices and methodologies and recommendations for planning, promoting, and implementing a unified effort between security domains. It is a planning model for merging parallel risk management processes, optimizing organizational alignment, and recommending training and performance measures.



INTERAGENCY SECURITY COMMITTEE

Items Prohibited in Federal Facilities

An Interagency Security Committee Standard

2022 Edition

U.S. Department of Homeland Security
Cybersecurity and Infrastructure Security Agency
Interagency Security Committee

Items Prohibited in Federal Facilities, An Interagency Security Committee Standard, 2022 Edition

This standard establishes guidance on protecting facility occupants and visitors from items which are dangerous, unlawful, or otherwise determined to create vulnerabilities in safety and security. Further, it establishes a list of prohibited items, as well as procedures to control these items, to increase consistency in security approaches and prevent confusion at screening checkpoints.

Updates in the 2022 edition include:

- Documentation requirements
- Inclusion of training aids as controlled items
- Prohibited Item Exception/Exemption Request Form

Risk Management Process for Federal Facilities, An Interagency Security Committee Standard

Appendix A: The Design-Basis Threat Report

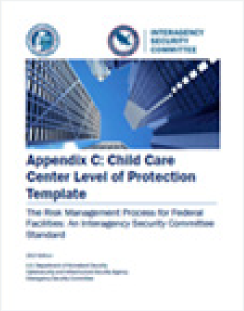
The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard

INTERAGENCY SECURITY COMMITTEE

Appendix B: Countermeasures

The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard

2021 Edition
U.S. Department of Homeland Security
Cybersecurity and Infrastructure Security Agency
Interagency Security Committee



INTERAGENCY SECURITY COMMITTEE

Appendix C: Child Care Center Level of Protection Template

The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard

Appendix A: The Design-Basis Threat (DBT) Report, 2022 Edition was updated by the DBT Subcommittee, in collaboration with the Argonne National Laboratory, utilizing the risk-utility model to determine baseline threat ratings.

Significant updates include:

- 11 Undesirable Event (UE) baseline ratings were increased,
- 12 UE baseline ratings were decreased, and
- An updated executive overview of threats to federal facilities portraying relative threats between UE categories and individual UEs.

Appendix B: Countermeasures, 2022 Edition, updated by the Countermeasures Subcommittee, focuses on a revision in the document's format. The Security Criteria tables have been substantially modified from previous versions. All information pertaining to each security criterion is now present on the same page, or consecutive pages, eliminating the need to jump between multiple pages within the document to view the additional details or applicable UEs.

Additional updates include:

- The Child Care Center baseline Level of Protection (LOP) is now annotated in the Security Criteria tables,
- The baseline LOP is only applicable until a risk assessment can be performed, and
- Risk acceptance can only occur after alternative risk mitigation strategies have been considered and documented.

Appendix C: Child Care Center LOP Template, 2022 Edition specifies the customized LOP to incorporate as the basis for Child Care Center security planning. It also presents implementation guidance for five potential scenarios, each representing the relationship between the Child Care Center and other federal facilities, including campus settings.

Users with a need-to-know may access these For Official Use Only (FOUO) appendices. To request access, email ISCAccess@hq.dhs.gov.

PROFILES IN EXCELLENCE

IRS Makes Strides with a Countermeasures Tracking Tool (CMT)

In FY 2022, the ***IRS Headquarters Security Division*** developed a ***CMT*** to provide a centralized and automated platform to track and manage countermeasure recommendations from security assessments and audit findings from FSAs, Facility Security Assessment Addendums, Facility Security Compliance Assessments, Treasury Inspector General for Tax Administration audits, and Government Accountability Office audits, as well as from internal reviews or audits. This tool also tracks funding and incorporates priority ranking.

The CMT facilitates real-time automated management of countermeasure recommendations—approved for accomplishment, denials, risk acceptance decisions, and the individual and collective costs.

Subcommittees and Working Groups

The ISC is a collaborative forum charged with enhancing the quality and effectiveness of security in and protection of federal facilities. The ISC does this by, with, and through its members within the primary governance frameworks of subcommittees and working groups, listed below. Participation on a subcommittee or working group is a significant, tangible way for ISC member department and agency personnel to actively contribute to the work of the ISC.

The ISC subcommittees are enduring bodies, while ISC working groups address a specific problem or task and are dissolved once the task is complete. If interested in participating, more information about the ISC subcommittees and working groups can be obtained by contacting the ISC inbox at isc.dhs.gov@hq.dhs.gov.

SUBCOMMITTEES

- Steering
- DBT
- Best Practices
- Convergence
- Standards
- Compliance
- Countermeasures
- Training

WORKING GROUPS

- Mail Handling
- Making the Business Case for Security
- Federal Mobile Workplace Security

PROFILES IN EXCELLENCE

Department of Health and Human Services (HHS) Leverages Partnership

The ***HHS, Program Support Center, Physical Security, Emergency Management, and Safety (PSEMS) Directorate*** is the HHS principal office responsible for providing physical security direction, oversight, and services. PSEMS invests heavily in ISC partnerships and processes, and the return-on-investment has been significant.

This year, HHS expanded a quarterly department-level working group, chaired by the PSEMS Director, by adding specific themes and messages, as well as external guest speakers from the ISC and other organizations, to reinforce standards, enhance partner engagement, and provide an added level of credibility to the forum. Additionally, HHS hosted the Office of Personnel Management's ISC Risk Management Process Training Course at the Hubert H. Humphrey Building, which was an opportunity to engage with over 35 personnel from seven partner agencies. PSEMS supports the Federal Risk Management Process Training Program (FRMPTP) by providing certified staff members to serve as training cadre. All PSEMS staff are required to attend FRMPTP as a pre-requisite to conducting site security assessments.

Finally, PSEMS provides staff to support the ISC Compliance Subcommittee and is ready, willing, and able to support future ISC projects. Ultimately, key investments in expertise, collaboration, and relationships established through these ISC forums enable a smaller-sized office like PSEMS to succeed at a larger-sized task of ensuring the safety and security of HHS employees, assets, and visitors. It is a team effort—an ISC model built for success.

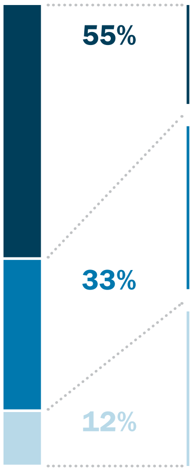
Training

The ISC continues to offer a variety of online and interactive training courses. The ISC's RMP and FSC Training provides an understanding of the ISC, the ISC RMP Standard, and the roles and responsibilities of FSCs. The course fulfills the necessary training requirements for FSC membership and is valuable for executives, managers, and personnel involved in making facility funding, leasing, security, or other risk-management decisions.

The RMP and FSC Training is instructor-led, provided by certified ISC staff, and includes ISC Regional Advisors who provide outreach and capacity-building to the 90 percent of government facilities located outside of the National Capital Region. Learning is scenario-based and includes knowledge checks, a practical exercise, and a rigorous examination to confirm learning objectives are met. The ISC offered 10 Virtual Instructor-Led Training courses graduating 268 students this year.

The ISC was excited to return to in-person training with deliveries sponsored by GSA in Fargo, ND; the Greater Kansas City Federal Executive Board (FEB) in Kansas City, MO; and GSA in Salt Lake City, UT.

RMP and FSC Training Attendance



Primary Members:

GSA, EPA, United States Department of Agriculture, Department of Veterans Affairs, Department of Justice, et al.

Associate Members:

National Institute of Standards and Technology, Administrative Office of the United States Courts (AOUSC), Pentagon Force Protection Agency, IRS, International Boundary and Water Commission, United States Secret Service, et al.

Non-Members:

National Oceanic and Atmospheric Association, Defense Contract Management Agency, Small Business Association, Centers for Disease Control and Prevention, and multiple private sector and state, local, territorial, and tribal organizations.

RMP and FSC Training Receives *96 Percent Approval Rating*

> ***"This course was fantastic and extremely helpful.*** *I wish I knew about it when I first started in the government and took on the FSC chair/Designated Official role 6 years ago."*

> *"I have been FSC chair for 2+ years and did not understand the level of responsibility each tenant agency has in the program.* ***I recommend this as a required training for all FSC participants*** *to help set expectations and ensure more active participation."*

> *"This training was organized, efficient, and well-presented. A very effective overview/starting point for knowledge in this area. The instructors were knowledgeable and accessible.* ***Great job—and thank you!"***

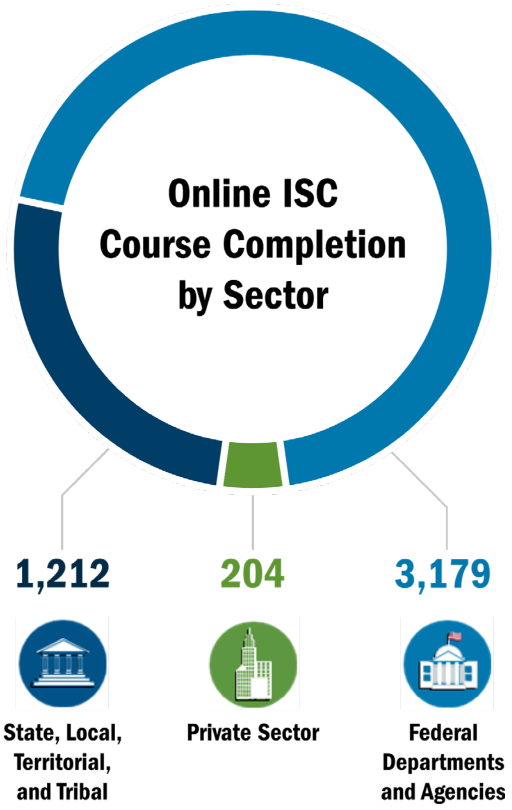
Online Training

The ISC also provides online training through FEMA's Emergency Management Institute. The online courses provide information on the ISC, its publications, and the Risk Management Process.

The courses include:

- **IS-1170:** Introduction to the ISC
- **IS-1171:** Overview of ISC Publication
- **IS-1172:** The Risk Management Process for Federal Facilities: FSL Determination
- **IS-1173:** Levels of Protection and Application of the DBT Report
- **IS-1174:** Facility Security Committees

The training can be found on FEMA's website. More information on ISC training can be obtained by contacting RMPFSCtrng@cisa.dhs.gov.



PROFILES IN EXCELLENCE

DOC Successfully Incorporates ISC Standards

DOC sustained its mission while also maintaining a safe environment for its staff. This was accomplished by utilizing the methods found in ISC standards and by layering in more effective systems and resources to protect DOC's personnel, assets, and mission.

- **Policy Push:** overhauled department-wide policies in the areas of information, personnel, and physical and operational security, which provided both department security personnel and our client base with the most accurate and effective security practices available to promote a safe and secure workplace.
- **Training:** required all employees within the 0800 Security Administration/Specialist Training Framework to complete FRMPTP, which ensures personnel have a foundational understanding of ISC standards and can execute the RMP at federal facilities.
- **Facility Security Assessments:** re-vitalized the FSA program to evaluate credible threats, identify vulnerabilities, and assess consequences in accordance with the ISC and DOC standards at DOC-owned/leased facilities, as well as select GSA-owned/leased facilities.
- **ISC Engagement:** maintained a consistent rate in ACES as evaluated by the ISC. DOC was third among organizations in the larger department/agency group and was fifth among all ISC members. DOC remains actively engaged through participation in ISC subcommittees and working groups, currently participating in six subcommittees and two working groups. A member of the DOC staff chairs the Making a Business Case for Security Working Group. Additionally, DOC hosted and assisted in the coordination of the September 2022 ISC Membership Meeting. Lastly, DOC participated as a host agency and verification team member for the ISC-CS Verification Pilot program in 2021.

Webinars

In addition to the RMP and FSC training, the ISC occasionally hosts webinars to better inform stakeholders on a variety of security related topics. In 2022, the ISC co-hosted a webinar with Homeland Security Today titled "Security Convergence: Achieving Integrated Security." The webinar drew attendance from over 330 federal and non-federal stakeholders and aligns with the ISC's guide of the same title published in 2022.

2022 'ASTORS' Honoring Government Excellence Award Winner

The ISC was honored to be chosen as the 2022 Platinum Award Winner at the American Security Today's Award Luncheon during the ISC East Conference held in New York City. The ISC was acknowledged for its RMP and FSC Training Program in the category of Best Federal Government Security Program, Excellence in Public Safety.

PROFILES IN EXCELLENCE

Federal Law Enforcement Training Centers (FLETC) Office of Security and Professional Responsibility (OSPR) Supports Hurricane Preparedness and Continuity of Training Operations

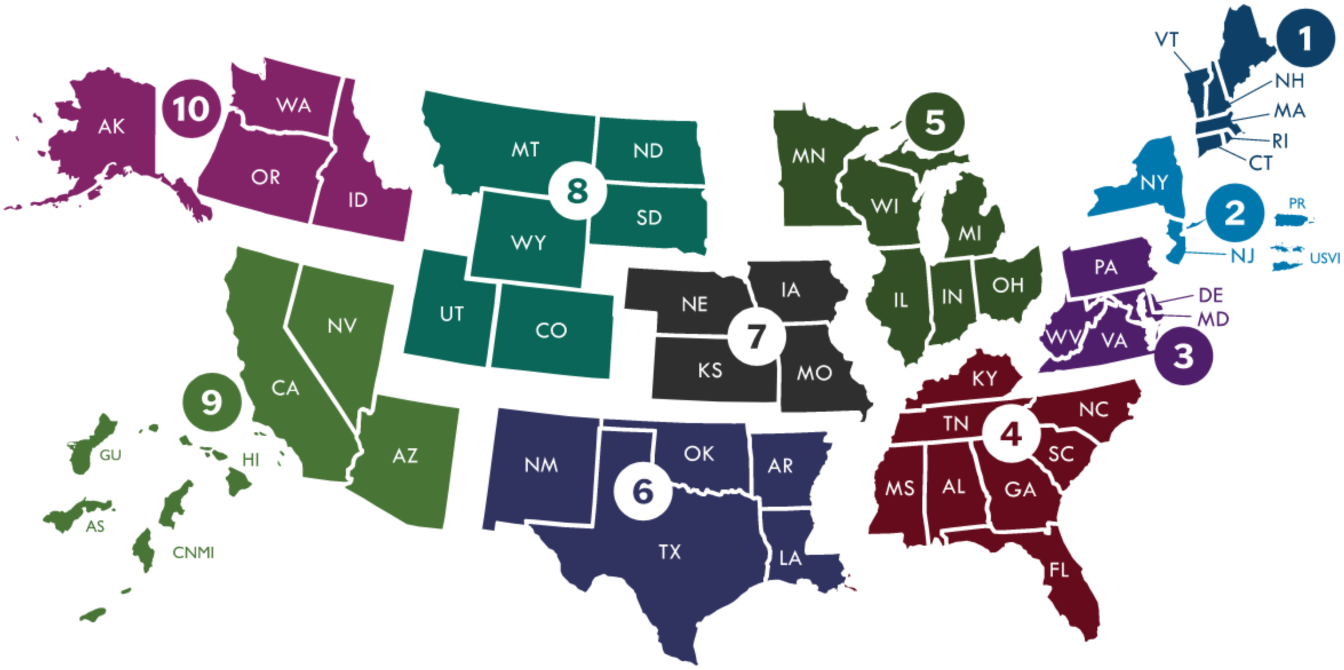
In response to Hurricane Ian's forecasted impact on two ***FLETC*** training delivery points, ***OSPR*** mobilized its resources to help prepare and safeguard FLETC's staff, students, contractors, and facilities in Glynco, GA and Charleston, SC. OSPR's law enforcement officers, security and emergency management specialists, and contract security professionals worked around the clock to support the evacuation of approximately 2,000 students from FLETC Glynco, prepared more than 400 Charleston students to shelter in place, maintained constant communication with key state and local public safety agencies, and provided emergency services throughout the event.

Following the storm, OSPR partnered with FLETC's Training Management Division and external stakeholders to expedite the arrival and intake of more than 2,200 returning and new students in less than 24 hours, allowing FLETC Glynco to reconstitute normal training operations almost immediately. Despite significant damage to buildings, powerlines, and some training venues at FLETC Charleston, no injuries were reported and training resumed almost immediately.

As the primary agency responsible for ensuring the security and integrity of FLETC, OSPR provides a full range of law enforcement, security, emergency management, and oversight services to FLETC's interagency training community.

Regional Advisors

ISC Regional Advisors serve as a regional resource to address ISC-related questions and concerns. They provide stakeholders in the field with a variety of advisory services including outreach, training, and general ISC support. Most of the Regional Advisor efforts focus on raising awareness of and training on ISC policies, standards, and recommendations, as well as communicating the importance of reaching federal facility security compliance. In 2022, ISC Regional Advisors delivered RMP and FSC training, delivered FSC seminars, attended and advised at FSC meetings, attended FEB meetings, provided subject matter expert support on ISC publications, maintained current relationships with key stakeholders, and forged new partnerships. Currently, there are five Regional Advisors serving 10 regions throughout the United States.



ISC REGIONAL ADVISOR CONTACT INFORMATION

CISA Region(s)	
1 2 3	**Joey Whitmoyer**
6 8	**C. Kevin Choate**
4	**Brian Pavone**
9 10	**Tony Evernham**
5 7	**Joe Lang**
National Capitol Region (NCR)	**Scott Dunford**

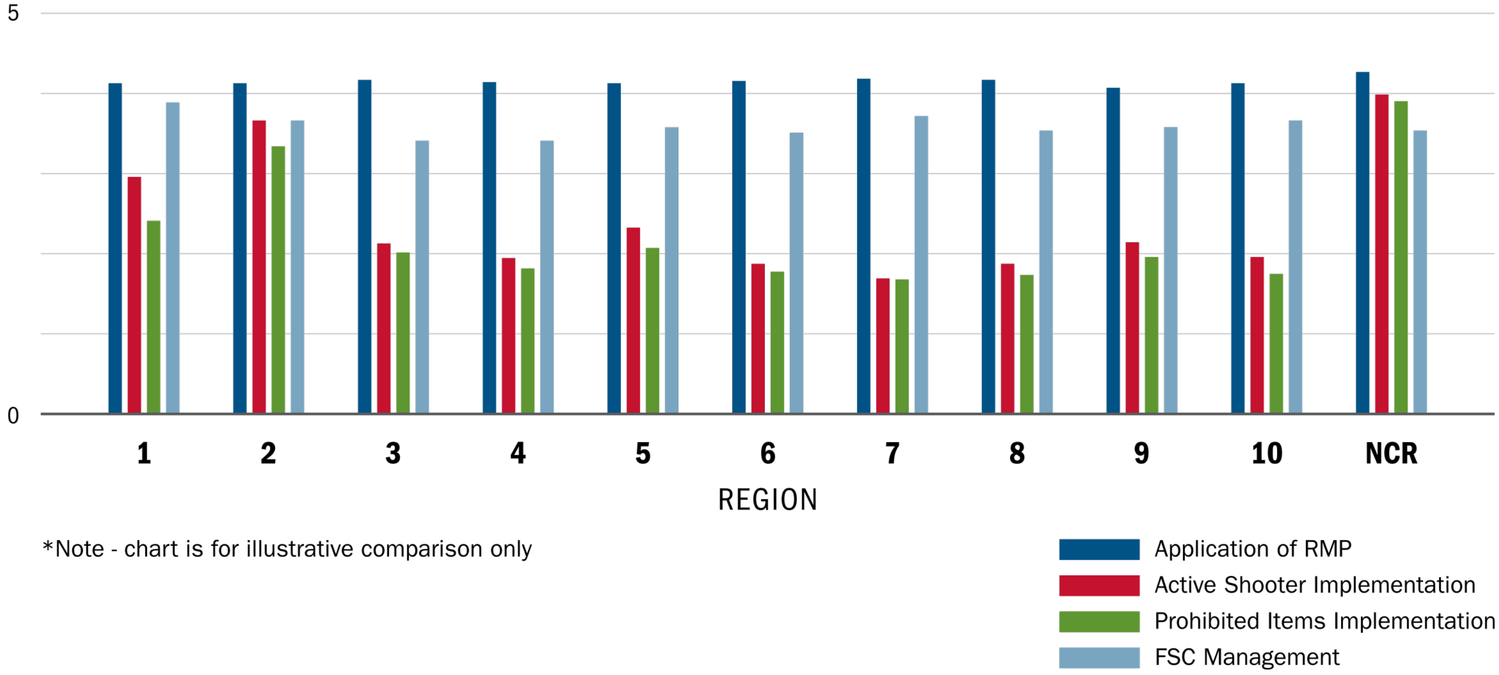
Facility-Level Compliance

As we continue to progress with verification and ensure facilities across the nation are protected to the same standard as intended by EO 12977, ISC Regional Advisors are a great resource for increasing facility-level compliance.

Beyond self-reporting and verification of compliance information, the ISC's Regional Advisors are available to assist with increasing the compliance with ISC policies and standards at the facility level. As referenced below, each region has varying levels of compliance with the core ISC policy and standards. There is still work to be done, especially in the areas of active shooter preparedness and implementation of the prohibited items guidance in federal facilities.

Regional Advisor contact information and regions serviced is located on the Regional Advisor Map. Additionally, region-specific information from each Regional Advisor can be obtained by registering for the Regional Distribution List.

Regional Review of 2022 Compliance Data



*Note - chart is for illustrative comparison only

GSA Enterprise Physical Access Control System (EPACS)

PROFILES IN EXCELLENCE

The ***GSA EPACS*** infrastructure is presently deployed at over 150 GSA-managed facilities, providing authenticated access to over 2,100 doors and over 200,000 federal employees and contract staff.

The GSA EPACS team assists GSA internally to comply with federal and agency guidance, directives, policies, and mandates for GSA-controlled space. GSA EPACS also provides subject matter expert support for FSCs and other agency inquiries as needed. The GSA EPACS team works closely with the United States Marshals Service, FPS, and AOUSC to deploy compliant integrated partnered solutions in courthouses.

Additionally, the GSA EPACS team provides subject matter expert level guidance and assistance to GSA customer/tenant agencies by reviewing their Physical Access Control System Scope of Work to help them achieve compliance with federal standards, policies, and directives.

Outreach

Strategic Communications and Outreach provides information and knowledge to inspire action. The key to effective understanding, utilization, and implementation of ISC standards is communication. The ISC facilitates a common level of understanding and shared information through a variety of Outreach and Communications channels.

Throughout the year, the ISC publishes quarterly newsletters, sends email communications, shares documents and resources, hosts annual meetings, maintains an active web presence, and conducts other outreach activities to allow all members to engage through a variety of modes: **one to one, one to many, and one to all.** In addition, members are encouraged to share their knowledge, successes, and challenges with their peers to facilitate information sharing and networking.

ISC Quarterly Newsletter

December 13, 2022
Issue 26

CISA.GOV/ISC
ISC.DHS.GOV@HQ.DHS.GOV

ISSUE HIGHLIGHTS

- Message from the Chair
- Member Spotlight: Government Facilities Sector (GFS)
- Compliance Data supports Regional Incident Response
- ISC 2022 Publications Overview
- Title 41, Part 102-81 Summary
- New Staff Alert: Meet the ISC's newest Regional Advisors
- ISC Training Schedule

Save the Date!

The next Membership Meeting will be on March 21, 2023.

Message from the Chair

It was great to see so many of you in-person at the Interagency Security Committee's (ISC) Membership Meeting on Tuesday September 30, 2022. I would like to thank the Department of Commerce once again for hosting and the Federal Bureau of Investigation, along with the National Capital Planning Commission, for their presentations which led to engaging, productive discussions.

Title 41 Part 102-81: Federal Management Regulation (FMR) Physical Security went into effect September 23, 2022. Title 41 Part 102-81 states each agency and Federal facility, operating under the jurisdiction, custody, or control of the General Services Administration (GSA), must comply with the policy and recommendations set forth by the ISC - this includes The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard (RMP Standard). More detailed information and resources can be found within this issue.

The work of the ISC is primarily done by, with, and through its membership. This includes the development of all publications through ISC Subcommittees and Working Groups and the recent releases of the Security Specialist Career Progression Guide: An Interagency Security Committee Guide, 2022 Edition, Appendix A: The Design-Basis Threat Report, 2022 Edition (FOUO), and Appendix B: Countermeasures, 2022 Edition (FOUO). I would like to thank and congratulate those who give of their time on our Subcommittees and Working Groups or otherwise contributed to these successful publications.

The validation window for submitting FY22 compliance information into the Interagency Security Committee Compliance System (ISC-CS) is open through December 15, 2022. Through compliance reporting, departments and agencies can analyze compliance with ISC policies and standards and are empowered to make defensible, risk-based, and resource-informed decisions to enhance security across the federal community.

Save the Date! The first Fiscal Year 2023 ISC Membership Meeting will be held on Tuesday, March 21, 2023, at USCIS HQC 5900 Capital Gateway Drive, Camp Springs, MD. USCIS has an amazing facility, and they are looking forward to sharing it with you. More information will be provided soon.

Finally, I would like to thank every member of the ISC for your continued support and engagement throughout this year. Have a wonderful holiday season.

Dr. David Mussington

Executive Assistant Director for Infrastructure Security

Cybersecurity and Infrastructure Security Agency (CISA)

NEW MEMBER HIGHLIGHT

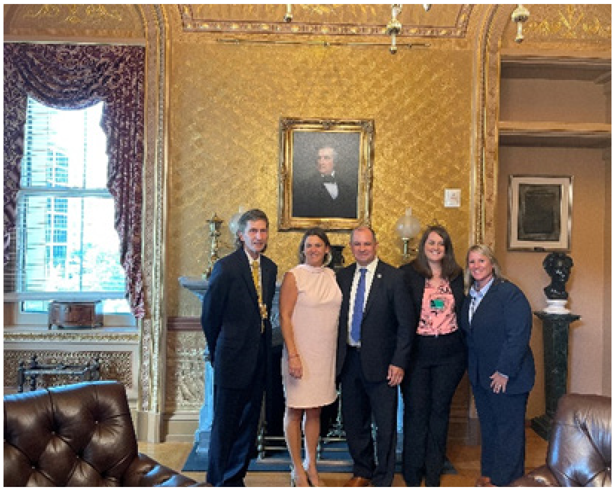
cfpb

The **Consumer Financial Protection Bureau** joined as an Associate Member in 2022.

Annual Meetings

Each year, the ISC invites each member to meet and discuss concerns, share best practices, and provide lessons learned from their organization with ISC leadership.

This year, the ISC hosted 56 annual meetings and 11 non-member meetings, which allowed the ISC to connect directly with its members and stakeholders. Annual meetings provide ISC leadership the opportunity to share updates on the Committee's collective work. These open discussions result in improvements to ISC publications, trainings, networking, subcommittee and working group participation, and connecting members to ISC Regional Advisors.



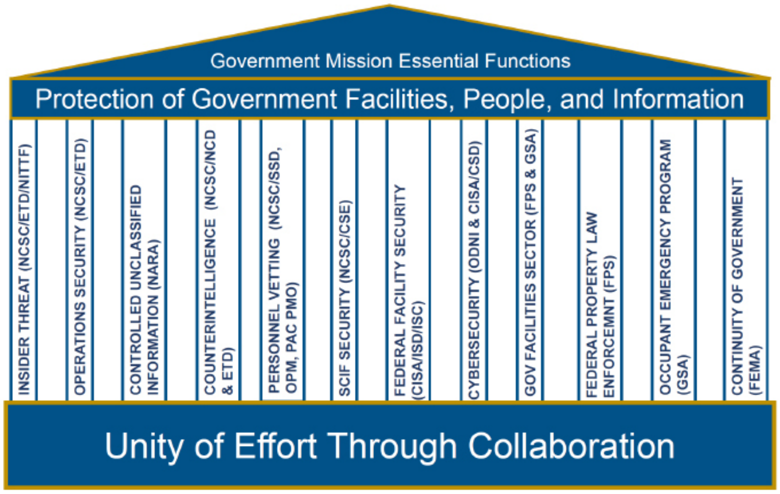
2022 Conferences and Speaking Engagements

Throughout 2022, the ISC participated in 13 security-related conferences throughout the country to share the work of the ISC. ISC staff and members served as subject matter experts on the topics of security convergence, unmanned aircraft systems, protecting federal facilities, and the ISC's RMP Standard.

In 2022, the main conferences the ISC supported were:

- Data Center Physical Security Working Group
- Global Security Exchange
- International Forced Entry Forum
- International Physical Security Forum
- National Homeland Security Conference
- Oklahoma City FEB Leadership Seminar
- Security Industry Association Government Summit
- U.S. Army Antiterrorism Seminar

In 2022, the ISC established the **Federal Security Protection Program Office** Roundtable to better integrate the mission spaces of federal security and protection program offices by developing a mechanism for formal collaboration.


Government Mission Essential Functions
Protection of Government Facilities, People, and Information
INSIDER THREAT (NCSC/ETD/NITTF)
OPERATIONS SECURITY (NCSC/ETD)
CONTROLLED UNCLASSIFIED INFORMATION (NARA)
COUNTERINTELLIGENCE (NCSC/NCD & ETD)
PERSONNEL VETTING (NCSC/SSD, OPM, PAC PMO)
SCIF SECURITY (NCSC/CSE)
FEDERAL FACILITY SECURITY (CISA/ISD/ISC)
CYBERSECURITY (ODNI & CISA/CSD)
GOV FACILITIES SECTOR (FPS & GSA)
FEDERAL PROPERTY LAW ENFORCEMNT (FPS)
OCCUPANT EMERGENCY PROGRAM (GSA)
CONTINUITY OF GOVERNMENT (FEMA)
Unity of Effort Through Collaboration

PROFILES IN EXCELLENCE

National Capital Planning Commission (NCPC)

The ***NCPC*** is the federal government's central planning agency in the National Capital Region and through its core activities including planning, policymaking, and project review, addresses current and emerging issues related to security. NCPC's Public Space Security Initiative is conducting place-based case studies and developing guidelines to address the evolving range of threats faced by people occupying public spaces.

On a larger scale, through the Pennsylvania Avenue Initiative, the agency is piloting strategies to support the long-term physical infrastructure (telecom, power, water, and security) needed to achieve the new vision for Pennsylvania Avenue as America's stage for nationally significant events, with modern infrastructure and comfortable and engaging public spaces to adapt to and accommodate daily activities and events. Results from these programs will be used to inform the updates to the Federal Elements of the Comprehensive Plan, a policy document used by NCPC to evaluate projects and plans for public spaces.

Additionally, NCPC's collaboration concerns issues related to public space and security. NCPC works closely with both federal and local stakeholders regarding the need for enhancing wireless communication infrastructure both around the National Mall and throughout downtown Washington, D.C. to ensure there is consistent design with limited impact on viewsheds, public spaces, and the monumental core. NCPC works with federal property owners on their perimeter security projects to incorporate design practices, preserve vibrant public spaces, and ensure security for individuals and physical assets.

Forging Ahead

COMPLIANCE

The compliance staff will use the results from the FY 2022 compliance reporting and lessons learned from verification in assisting ISC members to improve compliance. Additionally, the staff will work on improving the ISC-CS experience, developing data analysis tools, and assisting departments and agencies with refining their data in the ISC-CS.

The ISC will also be conducting the first year of compliance verification with ten verification reviews scheduled throughout 2023. The reviews provide an opportunity for ISC staff to provide additional compliance training and to further assist departments and agencies in improving their compliance scores.

The FY 2023 reporting requirements remain 100 percent of Organizational Benchmarks and 100 percent of Facility Demographic and Benchmark information.

POLICY, STANDARDS, AND RECOMMENDATIONS

In the next year, ISC subcommittees and working groups will continue to pursue publication of several guidance documents. Those anticipated for publication in 2023 include the Mail Center Security Guide, 5th Edition, and Making a Business Case for Security.

Furthermore, the ISC will be moving forward with the publication of Mobile Federal Workplace Security, after much collaboration and input from the ISC working group. By using a multitude of experiences and lessons learned from the ongoing COVID-19 pandemic, the working group is ready to publish a best practices document. This best practice guide will assist ISC members with implementing mobile federal workplace solutions for their workforce and facilities.

TRAINING

The ISC will continue to offer in-person and virtual training opportunities for the RMP and FSC training program. The first virtual training session was held in late January 2023 with numerous opportunities throughout the year.

Additionally, the ISC has developed and will be launching a new capacity building resource, the *Facility Security Committee Workshop*. This series is designed to educate and improve the capacity of the FSC's to carry out their duties and responsibilities. The workshop can be tailored to include any or all of the five available modules.

OUTREACH

In 2023, ISC staff will once again be reaching out to ISC members to connect for annual meetings either virtually or in-person. In addition, the ISC will continue to work on increasing its digital media presence using social media and updating the ISC website to reflect security-related events and news.

ISC Website:
https://www.cisa.gov/isc

General Inquiries:
ISC.DHS.GOV@hq.dhs.gov

Access FOUO ISC Publications:
ISCAccess@hq.dhs.gov

ISC Compliance:
ISCCS-Support@hq.dhs.gov

ISC Training:
RMP_FSCtrng@cisa.dhs.gov

Left: William S. Moorehead Federal Building, Pittsburgh, PA

Front Cover: Forest Service Building, Ogden, UT

Credit:
U.S. General Services Administration Historic Building Photographs