Interagency Security Committee

2023 Annual Review

February 2024

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

Message from the Chair

The unwavering devotion and hard work of the numerous public servants who uphold the safety and security of thousands of federal facilities throughout our country is critical in this dynamic threat environment. As we have seen, this year presented many challenges, obstacles, and threats to our federal facilities. I applaud Interagency Security Committee (ISC) members for addressing these risks and tangibly increasing security capacity across the federal government.

In November 2023, President Biden signed Executive Order (EO) 14111 to reinforce the importance of, and strengthen, the security of Executive Branch federal facilities. This EO strengthens and enhances the ISC's authorities to support its ongoing mission to improve Government-wide security for the Federal Executive Branch and strengthen the security of federal facilities in general.

The ISC has done an outstanding job of continuing to produce pertinent policy and standard guidance as well as taking the lead in establishing best practices for facility security. These accomplishments include the creation of numerous publications by the ISC working groups and subcommittees: ***Making a Business Case for Security: An Interagency Security Committee Best Practice***, ***General Services Administration (GSA) Mail Center Security Guide***, and updates to the ***Risk Management Process Standard Appendix A: Design-Basis Threat Report***, ***Appendix B: Countermeasures***, and ***Appendix C: Child Care Center Level of Protection Template Implementation Guidance***.

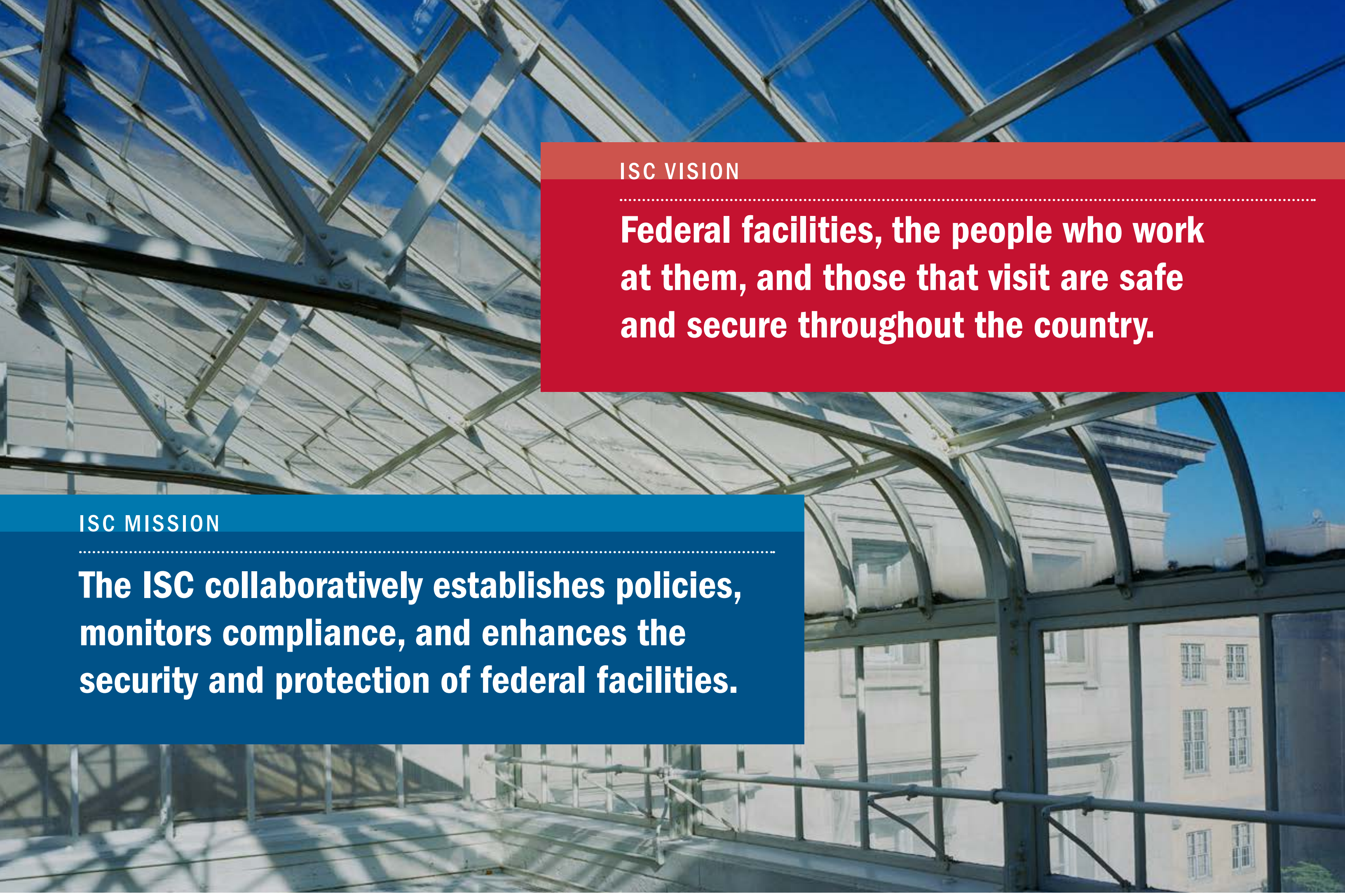
Compliance successfully implemented agency compliance verification and piloted facility compliance verification. Both organizational- and facility-level verifications are helping increase compliance levels and make reporting more informed. This year's compliance reporting continued to grow, to include 100 percent of our non-exempt members reporting.

In addition to the collective success of the committee, this ***2023 Annual Review*** continues our tradition of Profiles in Excellence, a compilation of contributions from ISC members that showcase the significant work of departments and agencies in the field. These member highlights demonstrate the areas where the ISC is leading the way in expertise and guidance, capacity building, assessments and analysis, and security operations. These entries are a true testament to the enduring strength and importance of the ISC.

Finally, I would like to express my gratitude to 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 furthering the ISC's mission and safeguarding all federal facilities, their employees, and visitors is commendable.

David Mussington, PhD

Executive Assistant Director for Infrastructure Security
Cybersecurity and Infrastructure Security Agency



ISC VISION

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

ISC MISSION

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

Table of Contents

Executive Summary

The Interagency Security Committee (ISC) 2023 Annual Review summarizes the ISC's commitment to providing its 66 members with education and excellence in federal security guidance, compliance assurance, training, and member outreach opportunities.

This year, the ISC witnessed a major milestone when President Biden signed Executive Order (EO) 14111. In the face of increasing threats to our government facilities, the Administration has reinforced the ISC's crucial role in establishing policies, monitoring compliance, and enhancing the security and protection of federal facilities. With this affirmation, the ISC eagerly looks ahead to working with its members and external stakeholders to strengthen the security of federal facilities.

In 2023, 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) trainings in numerous locations throughout the country, and hosted 55 annual meetings with ISC members.

This year's Annual Review includes significant accomplishments in the following categories: **Strengthening ISC Authorities; Compliance; Policies, Standards, and Recommendations; Training; Regional Advisors;** and **Outreach**. Furthermore, this publication highlights the important work of several ISC members by showcasing their commitment to enhancing the security and safety of our nations' federal facilities, workforce and the American citizens who visit them.

Below: *Seals and Logos of the 24 ISC Primary Members*
Previous and Next Page: *U.S. Post Office and U.S. Forest Service Building, Missoula, MT (details)*

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

Strengthening ISC Authorities

In 2023, the President further strengthened and supported the ISC's authority to enhance the security and protection of federal facilities by signing EO 14111 – Interagency Security Committee.

EO 14111 REINFORCES THE PRESIDENT'S COMMITMENT TO FEDERAL FACILITY SECURITY

Following the bombing of the Alfred P. Murrah Federal Building in Oklahoma City, President Clinton signed EO 12977 on October 19, 1995, creating the ISC.

While the federal security community has accomplished significant progress over the past twenty-eight years, the increase of ideologically motivated, violent extremists targeting government facilities has solidified the crucial function the ISC performs in establishing policies, monitoring compliance, and enhancing the security and protection of federal facilities.

Beginning in 2021, the National Security Council (NSC) led an interagency effort to strengthen the ability of the ISC to protect Executive Branch government facilities, those who work at them, and the American public who visit them. EO 14111 reaffirms and strengthens the government's commitment to protecting all federal facilities.

President Biden signed EO 14111 to reinforce the importance of, and strengthen, the security of Executive Branch federal facilities in the face of both persistent and emerging threats. In honor of the significance of the EO, the White House held a Signature Celebration Ceremony at the Eisenhower Executive Office Building on November 27, 2023.

EO Signature Celebration Ceremony
The White House, November 27, 2023

Top: *Caitlin Durkovich, National Security Council*

Bottom: *Nitin Natarajan, Deputy Director, CISA*

The major changes and impacts of EO 14111:

- Updated duties and responsibilities to better balance the ISC's authority with the central responsibility departments and agencies have for federal facility security.
- Added the requirement for the ISC to provide best practices for securing a mobile federal workforce.
- Added the requirement for the ISC 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 to raise visibility and accountability.
- Added the requirement for departments and agencies to designate a senior official responsible for implementation and compliance with the EO, and to support FSCs.
- Established minimum compliance monitoring requirements for the Department of Homeland Security (DHS), to include conducting risk-based compliance verification.
- Updated the definition of federal facilities to reduce ambiguity.

For more information on EO 14111, please visit the ISC's website: cisa.gov/additional-isc-resources.

PROFILES IN EXCELLENCE

The Internal Revenue Service Demonstrates Speed in Conducting Security Reviews

Beginning in August 2022, the Internal Revenue Service (IRS) responded to an increase of misinformation and false social media postings alleging weak security postures at its facilities, directing threats at IRS employees, and communicating anti-government threats in general. The IRS quickly reacted by performing a risk-based out-of-cycle security review. Utilizing the standards captured in ***ISC Appendix B***, the IRS physical security specialists reviewed an impressive total of more than 500 facilities within nine months. These reviews led to the development of numerous countermeasure projects ranging from administrative corrections to multi-year contracts addressing technology lifecycle issues.

Along with the out-of-cycle security reviews, the IRS extended random occupant screenings to more facilities and expanded communications to bring security awareness to IRS facilities nation-wide. Together with agency partners such as the Federal Protective Service (FPS), Treasury Inspector General for Tax Administration, the ISC and others, the IRS discussed the status of threats, the risk-based process, and developed and administered trainings on critical topics such as active shooter preparation and response, shelter in place, and other emergency scenarios to protect employees.

Today, with the guidance from the ISC, the IRS and its employees are better prepared and protected by these actions and continue to strengthen the security posture of IRS facilities across the country.

Compliance

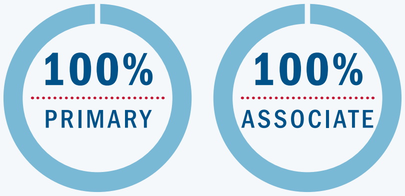
ISC members successfully completed the fifth year of compliance reporting. Compliance reporting provides ISC members with the means to measure, report, and analyze compliance with ISC policies and standards. This year was a continuation of last year's goal of reporting on 100 percent of organization benchmarks and 100 percent of facility portfolios.

Compliance reporting had immense support from ISC membership throughout the year. Over 350 attendees joined the five compliance Brown Bag trainings offered from May to October 2023. Additionally, during the 2023 reporting period, CISA support staff responded to over 315 compliance assistance requests, which included over 30 one-on-one system trainings.

Ultimately, 53 members and all non-exempt members reported in 2023. Additionally, ten 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.

There were 205 sub-organization benchmarks and 15,574 facility benchmarks completed and certified in 2023. The average organization compliance score maintained last year's level of 4.1 out of 5.0 while the average facility score increased from 3.6 last year to 3.7 this year.

Percentage of ISC Members Reported*



Excludes Exempt Members

Total Numbers Reported

205	Organization Benchmarks Submitted
15,574	Facility Benchmarks Submitted

Over 1300 additional facilities input from FY22

Average Compliance Scores

Organizational Score	**4.1 out of 5.0**
Facility Score	**3.7 (up from 3.6)**

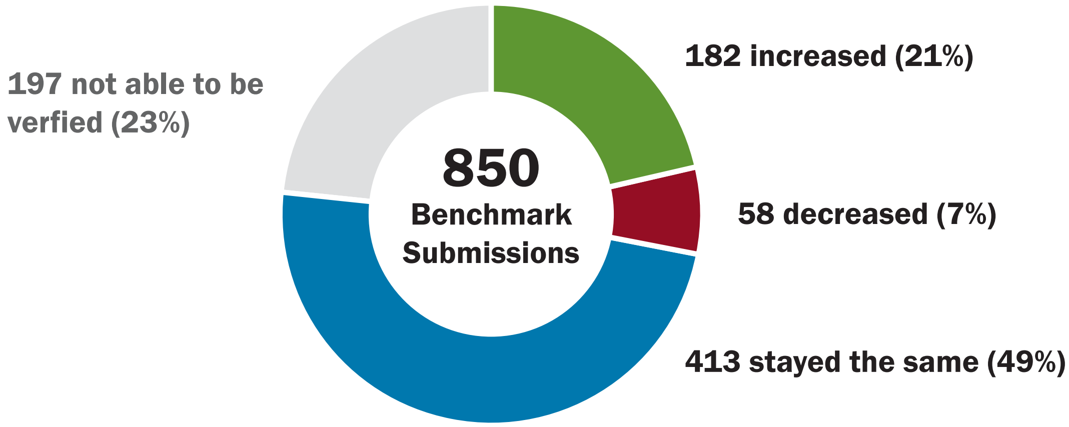
Org. compliance score remained the same in FY23. Facility score increased from 3.6

INAUGURAL YEAR OF COMPLIANCE VERIFICATION

In 2022, the ISC established Compliance Verification to provide an independent, third-party review of compliance at the organizational, sub-organizational, and facility levels. 2023 was the inaugural year of Compliance Verification. Verification reviews involve analyzing a department or agency's organizational documentation in support of their reported compliance data and providing recommendations on ways to improve compliance. Verification review teams verify the accuracy of member's compliance benchmark submissions, observe how the organization verifies compliance internally, analyze how the member implements ISC standards within governing documents and policies, and how the organization distributes and communicates the policy across the organization.

The ISC Compliance Subcommittee selects verification host organizations through risk-based selection criteria 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. Compliance Verification Reviews culminate with a formal report and out-brief to the organization that contains observations, recommendations, and best practices.

In 2023, the ISC completed ten compliance verification reviews. Verification review teams analyzed 850 benchmarks submissions. As the graphic below shows, the majority of benchmark submissions were verified as accurate responses and needed no change. However, the ISC did discover some benchmark questions where members were underreporting compliance and made recommendations to increase scores.



Finally, the ISC piloted facility verifications in 2023. This provided stakeholders with an opportunity to receive feedback and guidance on how to improve their compliance and ensure their facilities are secure.

The ISC notified 2024 Verification host organizations and scheduling is underway. For additional information or questions contact ISC-Verification@cisa.dhs.gov.

PROFILES IN EXCELLENCE

Cybersecurity and Infrastructure Security Agency Establishes New Organizational Policy

As part of its efforts to set the example for how organizations can address compliance with ISC standards, the Cybersecurity and Infrastructure Security Agency (CISA) issued its own internal policy signed by the CISA Director outlining how the organization will achieve compliance with ISC Standards. The Directive establishes the framework for ISC compliance and assigns responsibilities for making and documenting risk decisions, addressing security planning requirements such as developing an active shooter plan, an occupant emergency plan, and issuing a prohibited items list for each facility. This organizational approach to compliance ensures accountability for implementation of ISC processes and includes key stakeholders in planning to address countermeasure implementation.

The DHS Office of the Chief Security Officer commended this policy in its 2023 security performance assessment.

Policies, Standards, and Recommendations

The ISC's policies, standards, and recommendations lay the foundation for the work of the ISC and serve as a collaborative roadmap to protect federal facilities and those that work and visit them. With a current library of over 20 documents, the ISC is continually reviewing and improving its standards, policies, best practices, white papers, templates, and guides. This year, the ISC published five documents, three of which are For Official Use Only (FOUO) appendices within the *RMP Standard*.

2023 PUBLICATIONS

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

INTERAGENCY SECURITY COMMITTEE

Appendix A: The Design-Basis Threat Report

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

2023 Edition
U.S. Department of Homeland Security
Cybersecurity and Infrastructure Security Agency
Interagency Security Committee

Appendix A: The Design-Basis Threat (DBT) Report, 2023 Edition

The DBT Subcommittee updated *Appendix A* in collaboration with FPS and the Argonne National Lab (ANL), utilizing the risk-utility model to determine baseline threat ratings.

- Seven Undesirable Event (UE) baseline ratings increased.
- Six UE baseline ratings decreased.
- 36 sections received updates to the analytical basis, statistics, historic events, or other areas.

INTERAGENCY SECURITY COMMITTEE

Appendix B: Countermeasures

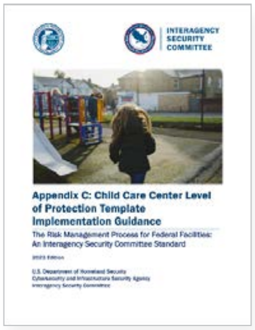
The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard

2023 Edition
U.S. Department of Homeland Security
Cybersecurity and Infrastructure Security Agency
Interagency Security Committee

Appendix B: Countermeasures, 2023 Edition

In an effort to maintain high-quality and accessible resources, *Appendix B*, updated by the Countermeasures Subcommittee, received significant updates to the layout and formatting to conform to a standardized ISC publication template. In addition to the formatting changes, an indexed list of Security Criteria has replaced the original table and reintroduced the numbering of the criteria along with links to the sections for improved user navigation. Additional updates include:

- Updated baseline Level of Protection (LOP) in accordance with updates from the UEs in the DBT.
- Removed references to Section 5 of the *RMP Standard* to align with the current edition.
- Updated the countermeasures for 14 Security Criteria.
- Updated Security Criteria details throughout the document.



INTERAGENCY SECURITY COMMITTEE

Appendix C: Child Care Center Level of Protection Template Implementation Guidance

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

2023 Edition

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

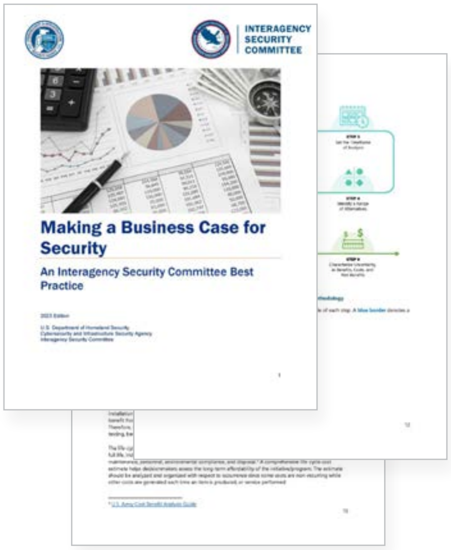
Appendix C: Child Care Center LOP Template Implementation Guidance, 2023 Edition

This past year, the ISC prioritized and addressed security at child care facilities, which led to a revision of its LOP template guide. *Appendix C* specifies the customized LOP to incorporate as the basis for child care center (CCC) security planning. It also presents implementation guidance for five potential scenarios, each representing the relationship between the CCCs and other federal facilities, including campus settings.

Users with a need-to-know may access these FOUO appendices.
To request access, email ISCAccess@hq.dhs.gov.

The National Labor Relations Board Revitalizes its Access Control System

The National Labor Relations Board (NLRB) began enhancement of security and efficiency of its access control system by establishing a centralized access control system for its regional offices. The centralized system bolsters security by providing a unified platform to manage and monitor access to critical resources. It also streamlines administration by simplifying the process of granting and revoking access privileges which reduces administrative overhead while meeting the requirements of Homeland Security Presidential Directive-12. The system's main control module is located at the NLRB headquarters, and it currently enables operators to control access to ten regional offices.



INTERAGENCY SECURITY COMMITTEE

Making a Business Case for Security

An Interagency Security Committee Best Practice

2023 Edition

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

Making a Business Case for Security, An Interagency Security Committee Guide, 2023 Edition

Increasingly complex security challenges and a dynamic threat environment necessitate the requirement for a strong and agile security planning, programming, and budgeting process. To that end, the Making a Business Case for Security Working Group developed *Making a Business Case for Security, An ISC Guide, 2023 Edition* to assist security professionals in constructing a decision-making process or rationale for proceeding with a security project or security program that enhances the security and protection of federal buildings and facilities, completing a benefit-cost analysis (BCA) to support spending decisions, applying these concepts to the ISC Risk Management Process, and measuring success. The guide also includes six common elements to making and delivering a successful business case for security and a companion Cost Analysis Template to assist organizations in calculating costs.

GSA

U.S. General Services Administration

Office of Government-wide Policy - Office of Asset and Transportation Management
Mail Management Policy

Mail Center Security Guide
5th Edition - 2023

Mail Center Security Guide, 5th Edition

The *Mail Center Security Guide, 5th Edition* serves as a comprehensive resource for departments, agencies, and component mail center managers in the administration of mail management programs. It represents the collaborative efforts of the ISC, General Services Administration (GSA), and federal mail professionals to consolidate GSA's ***Mail Center Security Guide, Fourth Edition*** published in 2014 and the ISC's ***Best Practices for Mail Screening and Handling Processes: A Guide for the Public and Private Sectors*** published in 2012, into a single resource.

SUBCOMMITTEES AND WORKING GROUPS

The ISC prides itself on being a collaborative forum that works by, with, and through its members within the primary governance frameworks of subcommittees and working groups (listed below). ISC member department and agency personnel actively contribute to the work of the ISC through their group participation. These opportunities allow individuals to share their expertise and perspectives that ultimately help improve security.

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

SUBCOMMITTEES

- Steering
- Best Practices
- Compliance
- Convergence
- Countermeasures
- Design-Basis Threat
- Standards
- Training

2023 WORKING GROUPS

- Mail Handling
- Making the Business Case for Security
- Federal Mobile Workplace Security *(Ongoing in FY 2024)*
- Occupant Emergency Plans *(Ongoing in FY 2024)*

PROFILES IN EXCELLENCE

The Mall Security Working Group Leans into Collaboration

The Mall Security Working Group (MSWG) was established in 2015 to provide a body for organizations with and cultural property institutions located on or near the National Mall to gather and share information on the protection of people, property, and assets during incidents and events. Since 2015 the MSWG has grown to include 60 organizations with more to be added in the coming year.

Similar to the ISC's mission, members of the MSWG prioritize cultivating a safe and secure environment around the National Mall. The National Archives and Records Administration, which is a MSWG primary member and member of the ISC, currently chairs the MSWG and hosts at least three meetings per year.

In 2023, the MSWG remained dedicated to providing a conduit for collaboration on protection matters, coordinating activities for upcoming events, capturing lessons learned, sharing threat information, exchanging best practices and training opportunities, and coordinating mutual aid when practical. The MSWG is a prime example of local cooperation and resourcing among local organizations with similar missions. In 2024, the MSWG will continue its mission of supporting physical security and encouraging knowledge sharing and cross-collaboration.

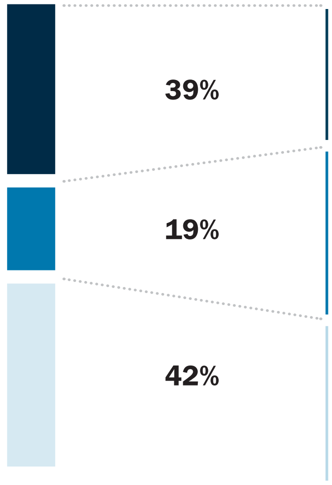
Training

The ISC continues to offer a wide range of online and interactive training courses. The ISC's RMP and FSC Training provides an understanding of the ISC, the ***RMP Standard***, and the roles and responsibilities of FSCs. Participants of the course gain valuable skills and knowledge in assessing and mitigating risks associated with facility funding, leasing, security, and other risk management decisions. In addition to fulfilling the necessary training requirements for FSC membership, the training equips participants with the necessary tools to make informed and effective decisions to ensure the safety and security of government facilities.

Certified staff, including ISC Regional Advisors (field personnel who provide outreach and capacity building to the 90 percent of government facilities located outside of the National Capital Region) present the RMP and FSC Training. The learning is scenario-based and there are comprehensive assessments to verify learning objectives. The ISC offered nine Virtual Instructor Led Training (VILT) courses, graduating **294** students.

We saw a 200 percent increase in in-person trainings delivered in 2023 with sponsorships from the Internal Revenue Service (IRS) in Covington, Ky.; the U.S. Environmental Protection Agency (EPA) in Duluth, Minn.; South Florida Federal Executive Board in Miami, Fla.; Federal Deposit Insurance Corporation in Arlington, Va.; Oklahoma City Memorial and Museum in Oklahoma City, Okla., and Snohomish County Public Utilities District in Everett, Wash.

RMP AND FSC TRAINING ATTENDANCE



Primary Members:

Department of Justice, U.S. Environmental Protection Agency, Department of Labor, Department of Interior, United States Marshals Service, Veteran Affairs, *et al*.

Non-Members:

Office of Natural Resources Revenue, U.S. Agency for Global Media, Bureau of Reclamation, Indian Health Service, Transportation Security Administration, Centers for Disease Control and Prevention, private sectors, state, local, territorial, and tribal organizations.

Associate Members:

Federal Bureau of Investigations, United States Citizenship and Immigration Services, United States Coast Guard, United States Secret Service, Internal Revenue Service, Customs and Border Protection, *et al*.

RMP AND FSC TRAINING RECEIVES 96 PERCENT APPROVAL RATING

> *"The instructors have extensive knowledge on the topics presented. Clear, and directed course material allowed me to follow along without issue."*

> *"Excellent organization, excellent presentation, and very knowledgeable trainers. Great experience and I appreciate all involved!"*

> *"The presenters did a great job in relaying the information, answering questions, and just the overall quality of the course. One of the best I have taken in quite some time."*

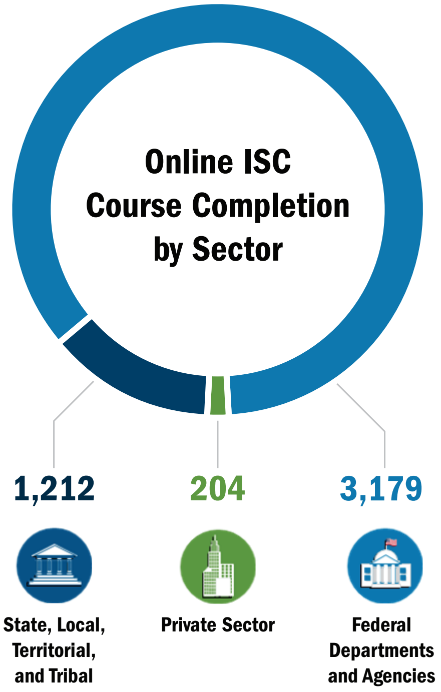
ONLINE TRAINING

The ISC provides online training through the Federal Emergency Management Agency's (FEMA) 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: Facility Security Level Determination
- **IS-1173:** Levels of Protection and Application of the Design-Basis Threat Report
- **IS-1174:** Facility Security Committees

The training is on FEMA's website. More information on ISC training is available by contacting: RMPFSCtrng@cisa.dhs.gov.



PROFILES IN EXCELLENCE

The U.S. Secret Service Strengthens Physical Security Program through Collaboration

The U.S. Secret Service (USSS), Security Management Division's – Physical Security Branch (SMD-PSB) coordinates, implements, and oversees the USSS Physical Security Program.

Within USSS SMD-PSB, the Facilities Security Section (FSS) develops and manages the agency's compliance with ISC security standards, to include the development, review, and update of facility security and active shooter response plans, as well as supporting facility security assessments, to ensure overall systems and processes are operating in compliance with national-level, DHS and USSS policies, requirements and/or standards.

SMD-PSB/FSS recently concluded an ISC Compliance Verification Review confirming 95% of its benchmark ratings with one acknowledged best practice for risk acceptance documentation. SMD-PSB is spearheading the agency's efforts to strengthen its physical security program thereby ensuring the safety and security of USSS facilities, assets, employees, and visitors. It is a truly collaborative effort to drive risk management and investment decision-making at both an enterprise and facility-specific level.

WEBINARS

The ISC often hosts webinars to coincide with the release of new publications to keep stakeholders informed on facility security topics. In April 2023, CISA support staff hosted, “Making a Business Case for Security” to assist security professionals in learning how to construct a decision-making process for proceeding with a security project or program, complete a BCA, apply concepts to the RMP, and measure success.

AWARDS

For the third consecutive year, the ISC’s RMP and FSC Training won the 2023 ‘ASTORS’ Homeland Security Award for Excellence in Public Safety. The RMP and FSC Training team earned a prestigious Platinum Award rating. American Security Today recognized the course for the proactivity and dedication its facilitators bring and for improving security practices to better protect facilities and the employees and public that visit them.

The DBT Subcommittee, in partnership with FPS and ANL won the 2023 ‘ASTORS’ Homeland Security Award for Excellence in Federal Government Security Program for development of an updated threat analysis methodology. The DBT Subcommittee also earned platinum honors. In 2022, the DBT Subcommittee created a Methodology Focus Group to evaluate the threat analysis model used in assigning threat ratings for each undesirable event profiled in the DBT Report. Leveraging an FPS partnership with ANL, the group conducted several lengthy online sessions to complete 54 value and objective elicitations. The Subcommittee then adopted a new risk-utility model. This new model redefined the two-objective model to a three-objective model including capability, history, and intentions, allowing for further depth of analysis and comparison of threats to federal facilities.

PROFILES IN EXCELLENCE

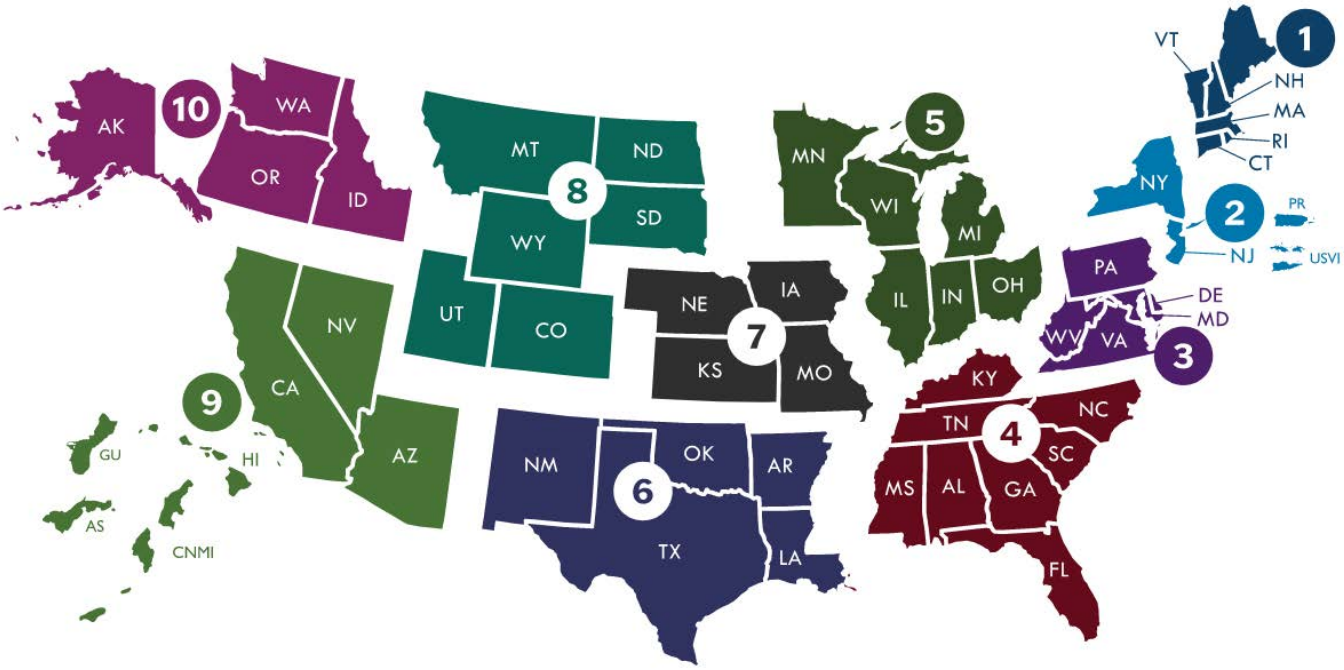
Vigilance and Modernization Fuels Department of Transportation’s Effective Security

The Department of Transportation (DOT) Office of Security continues to make significant progress in meeting, and in some areas exceeding, the ISC RMP Standard’s security requirements in the detection, prevention, and response to potential incidents and insider threats. By enrolling DOT employees and contractors in Record of Arrest and Prosecution Background as part of the Continuous Vetting process, it is now quicker and easier for the DOT Office of Security to detect, prevent, and respond to potential insider threats or workplace violence concerns. Implementation of enhanced cybersecurity measures, such as strong multifactor authentication protocols, helps to protect information systems from cyber-attacks.

DOT has substantially invested in upgrading its physical security systems to protect headquarter facilities from unauthorized access and theft, and to quickly identify potential threats before they happen. The Office of Security continues to explore and invest in new security technologies and procedures to stay ahead of the ever-evolving threat landscape.

Regional Advisors

The five ISC Regional Advisors (RAs), located across CISA's ten regional offices, continue to serve as a resource to address ISC and facility security-related questions and concerns. In 2023, the RAs delivered RMP and FSC trainings and FSC seminars, advised at FSC meetings, initiated a Cyber Tabletop Exercise, provided subject matter expert support on ISC publications, maintained current relationships with key stakeholders, and forged new partnerships with CISA Physical Security Advisors, FPS, General Services Administration, and the various Federal Executive Boards throughout the nation.



ISC REGIONAL ADVISORS

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

HOW REGIONAL ADVISORS SERVED ISC MEMBERS IN 2023

Outreach and Advisory Services

Technical or Compliance Assistance Visits Conducted
212*

States in which Federal Facility Stakeholders Visited
38

Federal Executive Board Meetings Attended
38*

FSC Seminars Delivered
6

FSC Meetings Supported
48

SLTT Engagements Supported
30*

Capacity Building

RMP & FSC Training – Regional Graduates
478*

ISC Focused Regional Programs Delivered
22*

ISC Program Support

Subcommittee or Working Group Supported/Led
8*

Organizational Compliance Verification Reviews Supported
5*

Draft ISC Documents Reviewed
31*

ISC Inbox Queries of FOUO Document Access Processed
231*

*Annual Goal Exceeded

Outreach

The ISC focuses its outreach on opportunities that enhance knowledge-sharing. Effective communication and member engagement remain a top priority of the ISC.

The ISC releases quarterly newsletters to promote new publications, provides the most recent training details, and shares updates on federal security events occurring across the country. The ISC aims to disseminate the latest resources and documents via email, TRIPwire, and other channels to ISC members and stakeholders. To enable participation from all members, the ISC also organizes annual meetings and membership meetings to encourage participants to share best practices, successes, and challenges with peers as well as facilitate information sharing and networking.

ANNUAL MEETINGS

Annual meetings provide a forum for interactive dialogue between CISA support staff and members to address federal facility concerns, share best practices and resources, exchange lessons learned, and communicate updates on the Committee's collective work. These open discussions result in improvements to ISC publications, trainings, enhanced interagency networking, along with subcommittees and working group participation. This year, the ISC was thrilled to have the opportunity to host **55 annual meetings** and **six non-member meetings** both in-person and virtually.

MEMBER MEETINGS

The ISC hosted three member meetings, engaging with members on key ISC updates and specialized federal facility security topics designed to share knowledge and communicate best practices. In 2023, the ISC conducted these meetings at the headquarters of the U. S. Citizenship and Immigration Services (USCIS), the Federal Aviation Administration (FAA), and IRS.

During these meetings, the ISC briefed members on program updates, best practices, publications, and compliance verification. Each gathering, the ISC focused on a priority and topic relevant to its members. At USCIS, FEMA detailed its disaster response efforts and site selection process of disaster recovery centers and facility risk assessments. While at FAA, FPS offered guidance to a recently released *ISC Standard: Items Prohibited in Federal Facilities*. Lastly, during the final FY 2023 Membership Meeting at the IRS, the organization provided a detailed brief on its facility risk and priority register process and the GSA reviewed updates to a publication developed with the ISC on mail handling.

Member Meeting Survey
Thank you for attending ISC September 2023 Membership Meeting!
Please scan the QR code below to complete a quick survey.

2023 CONFERENCES AND SPEAKING ENGAGEMENTS

Throughout 2023, the ISC participated in numerous security-related conferences throughout the country and shared the latest resources produced by ISC subcommittees and working groups. CISA support staff and members served as subject matter experts on the topics of making a business case for security, the success of the compliance program, protecting federal facilities, and the ISC's ***RMP Standard***.

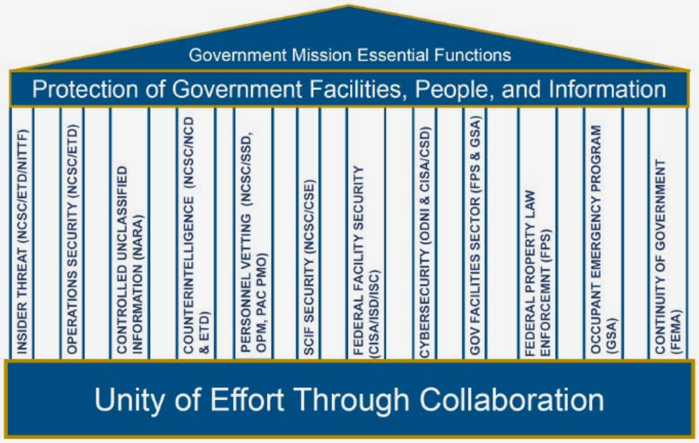
In 2023, the main conferences the ISC supported were:

- Critical Infrastructure Protection and Resilience, North America
- International Forced Entry Forum
- National Homeland Security Conference
- Security Industry Association Government Summit
- Security Industry Association International Security Conference and Exposition, West
- U.S. Army Antiterrorism Seminar

New Member Highlight

Supreme Court of the United States Police

LEARN MORE



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

Established in 2022, the Federal Security Protection and Program Offices (FSPPO) Roundtable serves as an opportunity to collaborate on the development of policies and share security program implementation best practices. The FSPPO Roundtable most recently met in April 2023 at CISA's Courthouse location and held discussions to build relationships, leverage knowledge, and close information gaps.

Forging Ahead

COMPLIANCE

The ISC will use the results from the FY 2023 compliance reporting and lessons learned from verification in assisting ISC members to improve compliance. Additionally, the team will work on focused organizational and member assistance in 2024 and will continue assisting departments and agencies with refining their data in the ISC-CS. The ISC will be introducing a few new benchmark questions in 2024 and will message this out to users.

The ISC will also be conducting the second year of compliance verification reviews. The reviews provide an opportunity for the ISC to further assist departments and agencies in improving their compliance scores.

The FY 2024 reporting requirements remain 100 percent of Organizational Benchmarks and 100 percent of Facility Demographic and Benchmark information.

POLICY, STANDARDS, AND RECOMMENDATIONS

The ISC migrated its publications including FOUO documents from the Homeland Security Information Network to TRIPwire to consolidate all content in a single location. The ISC team will assess user experience in FY 2024.

ISC subcommittees and working groups will continue to pursue publication of several guidance documents. Those anticipated for publication in 2024 include the ***Federal Mobile Workplace Security***, the ***Risk Management Process Standard***, ***Occupant Emergency Programs***, ***Resilience in Convergence***, ***Updated Compliance Benchmarks***, and ***Managing Risk of Adverse/Involuntary Employee Separations***.

TRAINING

The ISC will continue to offer both in-person and virtual training opportunities for the RMP and FSC training program. The next virtual training session will be on February 22, 2024, with additional opportunities throughout the year.

Additionally, the ISC will be conducting quarterly in-person RMP and FSC trainings within the National Capital Region (NCR), the first of which was on November 30, 2023, at the ISC headquarters. The ISC will announce future NCR training dates by email and posts on the ISC's public facing website.

OUTREACH

The ISC will continue to maximize engagement with membership through in-person and virtual annual meetings. The team will be revisiting the cadence and styles of newsletters and will be open to promoting members' facility physical security news. Additionally, the ISC will explore opportunities to increase its digital media presence using social media and updating the ISC website to reflect security-related events and news.

ISC Website:
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: *J. J. Pickle Federal Building, Austin, TX*

Front Cover: *U.S. Post Office and U.S. Forest Service Building, Missoula, MT*

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