

ISC Quarterly Newsletter

August 22, 2022
Issue 25

[CISA.GOV/ISC](https://cisa.gov/isc)

ISC.DHS.GOV@HQ.DHS.GOV



ISSUE HIGHLIGHTS:

- Message from the Chair
 - Security Convergence: Achieving Integrated Security, An Interagency Security Committee Standard Best Practice, 2022 Edition Published
 - Items Prohibited in Federal Facilities: An Interagency Security Committee Standard, 2022 Edition Published
 - Executive Order (EO) 12977 Update
 - Release of ISC FOUO Material
 - ISC Training Schedule
- June Membership Meeting:
September 20, 2022



Message from the Chair

This spring, the United States continued to face a diverse and challenging environment of several threat vectors. I would like to take this opportunity to thank every Interagency Security Committee (ISC) member for their continued dedication to enhancing the security in and protection of buildings and facilities in the United States occupied by Federal employees and visitors for nonmilitary activities.

First, I would like to remind everyone the ISC Compliance System (ISC-CS) is open for Fiscal Year 2022 (FY22) reporting and you may access the system at: <https://isccompliance.dhs.gov/>. Compliance reporting provides ISC members with the means to measure, report, and analyze compliance with ISC policies and standards. Compliance with ISC standards and policies empowers federal departments and agencies to make timely and informed decisions that are defensible, risk-based, and resource-informed to enhance security across the federal community. Monitoring compliance via the ISC-CS allows users to identify areas to focus their efforts individually and collectively. ISC compliance data also provides a resource for member departments and agencies to demonstrate their compliance with ISC standards and policies to government oversight entities.

In June 2022, the ISC released [Items Prohibited in Federal Facilities: An Interagency Security Committee Standard, 2022 edition](#). This document establishes updated guidance for prohibited items in federal facilities. Thank you to each member of the ISC who contributed their time and expertise to updating this document.

On June 28, 2022, ISC staff conducted the [Risk Management Process \(RMP\) & Facility Security Committee \(FSC\) Training](#) in Fargo, N.D. This is the first in-person training the ISC has conducted in two years. The next RMP & FSC in-person training will take place in Kansas City, Mo., on September 29, 2022.

Lastly, Executive Order (EO) 12977 is currently undergoing an update. We anticipate the updated EO will be released in Fall 2022. The updated document will ensure the ISC is postured to address the shifting threat environment for at least another 25 years.

As a reminder, the next ISC Member meeting will be held in-person **Tuesday, September 20, 2022 from 10 AM to Noon ET at the Herbert C. Hoover Building, 1401 Constitution Ave. Northwest, Washington D.C. 20230**. I look forward to seeing you all there!

Again, thank you to every member of the ISC for your continued support and engagement.

Dr. David Mussington
Executive Assistant Director for Infrastructure Security
Cybersecurity and Infrastructure Security Agency (CISA)

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

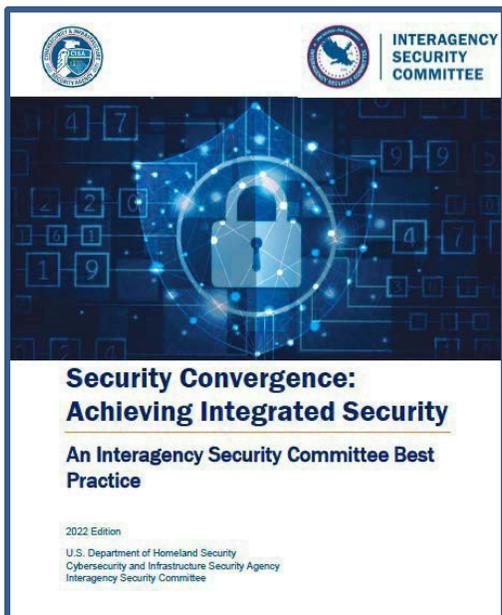
By ISC Staff

In March 2022, the ISC released [Security Convergence: Achieving Integrated Security, An Interagency Security Committee Standard Best Practice, 2022 Edition](#).

This document assists organizations seeking to achieve integrated security through a collaborative effort between physical security, information security, cybersecurity, information assurance, and information technology to protect assets. It provides:

- Guidance to assist federal executive branch departments and agencies in achieving integrated security through best practices and methodologies.
- Recommendations for planning, promoting, and implementing a unified effort between several related areas, including information security, physical security, cybersecurity, and information technology.
- A planning model for the merging of parallel risk management processes, the optimization of organizational alignment, as well as recommended training and performance management.

If you have questions, please email ISC.DHS.GOV@HQ.DHS.GOV



Items Prohibited in Federal Facilities: An Interagency Security Committee Standard, 2022 edition Published

By ISC Staff

On June 1, 2022, the ISC released its update of [Items Prohibited in Federal Facilities: An Interagency Security Committee Standard, 2022 edition](#) to establish guidance to protect facility occupants and visitors from items that are dangerous, unlawful, or otherwise determined to create vulnerabilities in safety and security. Further, it establishes a list of prohibited items and procedures to control them, increasing consistency in approach and preventing confusion at screening checkpoints.

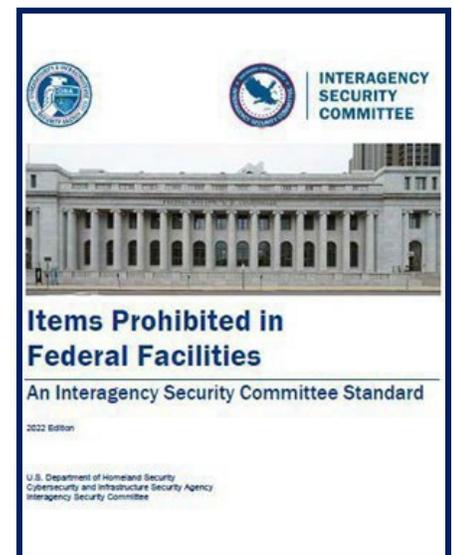
Updates in the 2022 version include:

- Documentation requirements
- Inclusion of training aids as controlled items
- [Prohibited Items Exemption Request Form/Template](#)

Consistent with Executive Order (EO) 12977, *Items Prohibited in Federal Facilities: An Interagency Security Committee Standard*,

identifies a baseline list of prohibited items that each responsible authority shall customize to mitigate facility risk. It is applicable to all executive branch buildings and facilities in the United States occupied by federal personnel for non-military activities. These facilities include currently owned, to be purchased, or leased facilities; standalone facilities; federal campuses; and, where appropriate, individual facilities on federal campuses and special-use facilities. Additionally, per Department of Defense (DoD) Instruction, 2000.12, all DoD leased facility space or space in buildings owned or operated by the U.S. General Services Administration (GSA) not located on DoD property must comply with this standard.

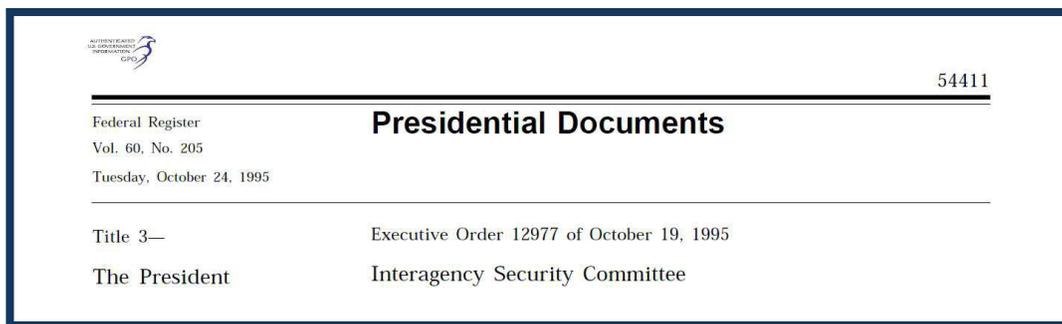
For more information about the ISC, please visit the [ISC home page](#).



Executive Order (EO) 12977 Update

By ISC Staff

EO 12977 was signed October 19, 1995 following the bombing of the Murrah Federal Building and established the ISC to address the vulnerability of federal facilities. Besides minor updates in 2003, EO 12977 has remained unchanged since its inception. Although much progress has been accomplished over 25 years, the threat environment has shifted, and Federal Facilities are now more vulnerable than ever. The increase of civil unrest and ideologically motivated violent extremists has solidified the crucial function the ISC performs in establishing policies, monitoring compliance, and enhancing the security and protection of Federal facilities. These changes necessitated a refresh of EO 12977.



A Sub-Interagency Policy Committee (Sub-IPC) was established in 2021 with members from 26 executive branch departments and agencies with the objective to:

- Update duties and responsibilities to better reflect the limits of the ISC’s authority and responsibility
- Clarify the definition of and applicability to federal facilities
- Clarify the ISC’s responsibilities to “monitor compliance”
- Update to the “Cooperation” subsection to address systemic barriers to compliance

Beginning in July 2021, the ISC staff facilitated nine Sub-IPC meetings where Sub-IPC member inputs were discussed and reviewed by the members. At the conclusion of the Sub-IPC the members had agreed on several changes to the EO including:

- Updated federal facilities definition to reflect their contemporary nature (e.g., Government Owned, Contractor Operated (GOCO) facilities)
- Added requirements for ISC to provide best practices for securing a mobile federal workforce
- Instituted a biennial summary report detailing compliance results to the Director of the Office of Management and Budget and the Assistant to the President for National Security Affairs
- Required departments and agencies to designate a senior official responsible for implementation and compliance of the EO and ensure support for FSCs
- Clarified the ISC’s responsibility to “monitor compliance” by defining its components to include maintaining benchmarks, requiring periodic reporting, specifying who is required to report, and conducting risk-based compliance verification
- Added a “Scope” section including key definitions for Executive Agency, Federal Facilities, Federal Employees, Federal Contractors, and Facility Security Committee

The updated EO recently completed review by the Homeland and Critical Infrastructure Resilience IPC and is currently being reviewed by National Security Committee Legal. Barring any major concerns, the EO will then move to the Deputies Committee. While a final signing date for the updated EO has not been determined, the Sub-IPC member’s inputs will ensure the ISC is postured to address the shifting threat environment for at least another 25 years.

Release of ISC FOUO Material

By ISC Staff

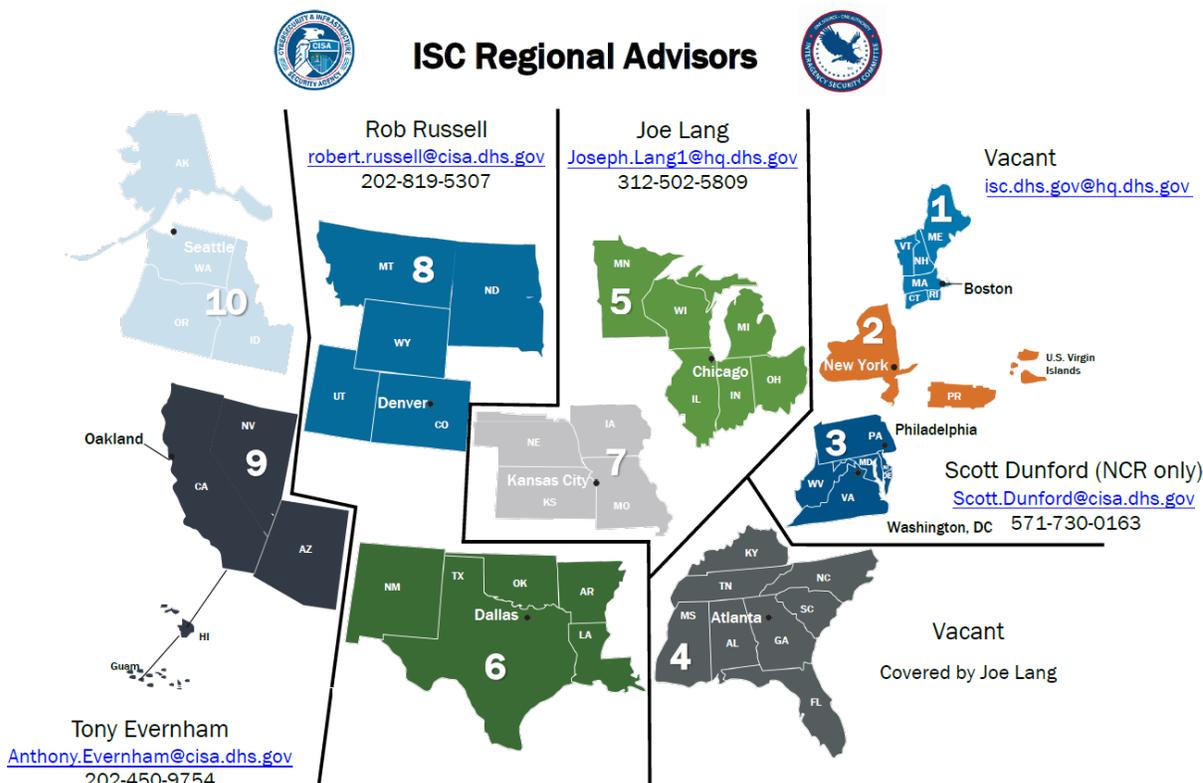
FOR OFFICIAL USE ONLY

Private contractors or consultants working on government projects often request ISC “For Official Use Only” (FOUO) documents such as the Risk Management Process for Federal Facilities: An Interagency Security Committee Standard, Appendix B: Countermeasures. However, prior to the release of FOUO material, the ISC must receive a formal request from the Contracting Officer Representative (COR) with detailed information including the contractor’s information, a “need-to-know” statement, length/term of access to the material, and the specific FOUO document(s) requested.

When the formal request is received, a member of the ISC staff will validate the information with the COR and request the COR to execute a Non-Disclosure Agreement with each person requesting the material. Once complete, the ISC staff will send the documents directly to the COR for further approved distribution. The ISC will not send documents to non-government emails.

If you have any questions or would like to request a copy of the FOUO Request Information Template, send an email to ISC.DHS.GOV@HQ.DHS.GOV with the subject “ATTN: Release of information request”.

Additionally, your ISC Regional Advisor (RA) can assist you with FOUO requests or any other ISC-related matters such as outreach, training, providing advisory services, answering compliance and facility-specific questions, and serving as a resource for all ISC-related questions and concerns. See the regional advisor map to identify your RA.



Upcoming ISC Trainings

The ISC continues to offer its award-winning training virtually and in-person. To request and schedule in-person training, please see the available dates and send an email to RMP_FSCtrng@cisa.dhs.gov for more information: (in-person training dates are on a first come first serve basis). In addition to the RMP training, later this year the ISC will begin piloting FSC Workshops. If you are interested in participating in an FSC Workshop Pilot, please contact us at the email above. For more information about the course or how to register visit the [ISC Training web page](#).

In-Person RMP & FSC Training

This half day (5 hours), instructor-led training course, serves as a prerequisite for FSC membership, covers the ISC RMP and the roles and responsibilities of FSC members. Successful completion of this management level course – MGT 909 – will earn graduates 0.3 CEUs (Continuing Education Units) through the course’s accreditation with the International Association for Continuing Education and Training (IACET). The target audience includes FSC Chairs, FSC Members, Executives, Managers, and any personnel involved in making facility funding, leasing, security, or other risk management decisions. There are no prerequisites for this course, and it is offered at **no cost to participants**. This training may be taken in-lieu-of the online Homeland Security Information Network (HSIN) courses (IS-1170-1174) and provides an opportunity for students to engage with ISC staff and to learn in an interactive environment with their peers. Dates are provided on a “first come first serve basis” for Departments and Agencies to schedule In-Person RMP & FSC Training at their location. Departments and Agencies must complete the “In-Person Training Request Form” in order to schedule their training and submit to RMP_FSCtrng@cisa.dhs.gov please reach out to your Regional Advisor or ISC Training Staff at RMP_FSCtrng@cisa.dhs.gov for any questions. For additional training options please see the Federal RMP Training Program dates offered by the Office of Personnel Management (OPM).

RMP & FSC- VILT Start Time	Upcoming CY22 Training Dates
9 AM Eastern Time	October 18-19, November 8-9
9 AM Central Time	September 13-14
9 AM Mountain Time	August 23-24

In-Person Training Dates available for Department and Agencies to request:

- August: 9, 11, 30
- September: 27, 29
- October: 4, 6, 25, 27
- November: 1, 3

Department/Agency Student Registration Requirements: Minimum of 30 and Maximum of 45