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 20, 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 proudly 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 Ladder: 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)

ISC Member Spotlight: Government Facilities Sector (GFS)

By GFS Staff -

The GSA and the Federal Protective Service (FPS) partner to co-lead the Government Facilities Sector. The GFS is one of the nation's 16 critical infrastructure sectors bringing together Federal, State, Local, Tribal and Territorial (FSLTT) government stakeholders to help protect personnel, facilities, systems, and assets, as well as the essential functions they perform. The GFS brings together partners ranging from senior officials to agency staff across multiple disciplines, including security (cyber-physical), law enforcement, military, education, emergency management and health care professionals, performing a variety of functions with a shared goal of building national security and resilience using an all-hazards, all-threats approach. Through collaboration the GFS promotes relationship-building, information-sharing, and coordination.

Collectively, the GFS constitutes one of the largest and most complex of the 16 critical infrastructure sectors. The GFS comprises three subsectors: the Education Facilities (EF) Subsector, led by the U.S. Department of Education; the Election Infrastructure (EI) Subsector, led by the Cybersecurity and Infrastructure Security Agency's, National Risk Management Center; and the National Monuments and Icons (NMI) Subsector, led by the U.S. Department of Interior. With more than 900,000 constructed assets owned or operated by the Federal Government alone, the sector includes assets owned or operated by the 56 States and territories, 3,031 counties, 85,973 local governments, and 566 Federally recognized tribal nations.

GSA and FPS continually collaborate with the sector, across sectors with interdependencies (such as the Emergency Services Sector) and partners (such as the ISC) across the whole of government to:

1. Be fully responsive to the needs of the sector.
2. Gather and provide critical information, analysis, and resources.
3. Host and participate in meetings and webinars addressing the key risks and related risk management strategies.

Government practitioners can discover invaluable partners; receive critical information and resources; and hear from subject matter experts (SMEs) across the government to help strengthen protection, prevention, mitigation, response, and recovery actions from an all hazards, all-threats perspective.

To join and become a member of the GFS, please email NIPP-GFS@fps.dhs.gov We look forward to working with you.

Compliance Data Supports Regional Incident Response

By ISC Staff

ISC Regional Advisors are integrated with the Cybersecurity and Infrastructure Security's (CISA) regional offices. Across the nation, CISA regional staff offer a range of cyber and physical services to support the security and resilience of critical infrastructure owners and operators and FSLTT partners. In addition to their roles of providing compliance assistance and conducting outreach, regional advisors support the preparation, response, and recovery efforts for hazards impacting critical infrastructure throughout their assigned regions. One of the ways they support this effort is by identifying federal facilities and critical infrastructure that can potentially be impacted by incidents such as wildfires, hurricanes, and earthquakes.

ISC Regional Advisor Tony Evernham recently collaborated with CISA regional operations personnel in region 9 to create a Global Information Infrastructure (GII) map layer utilizing facility demographics information captured in the ISC-CS. Regional staff utilize the data internally to plot locations of known federal facilities and recall this information when preparing for, or responding to, natural hazards or man-made threats.

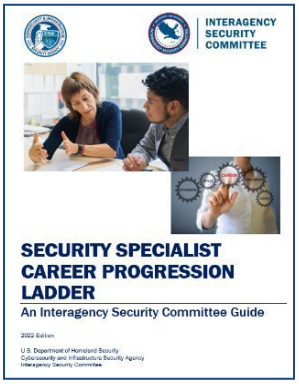
Member Participation Equals Results for ISC’s Policies, Standards, and Recommendations

By ISC Staff

The ISC’s Policy, Standards, and Recommendations (PSR) lays the foundation for the ISC work that serves as a collaborative roadmap to protect federal facilities and those that work at and visit them. Executive Order 12977 established the ISC and gave it three responsibilities:

Establish Security Policies **Ensure Compliance** **Enhance Effectiveness**

Everything done by the ISC is by, with, and through the members. Member participation through the ISC’s 22-step publication process is necessary to meet these responsibilities. The process, which consists of six phases: approval, forming, development, review, edit, and publish provides six touchpoints where members can have input to the various documents the ISC publishes. Whether actively participating in a subcommittee or working group, critically reviewing documents, providing feedback, or suggesting topics for membership meetings, member collaboration is critical to the success and effectiveness of the ISC.


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

Recent publications include:

Security Specialist Career Progression Ladder 2022 Edition: This document is intended to be a companion to the *Security Specialist Competencies: An Interagency Security Committee Guide*. It provides a methodology and resources on how to advance security specialist knowledge and skills, identify existing knowledge gaps, and progress as well-rounded security professionals. The guide also assists supervisors and employees in discussions on professional development. Key areas that this document will assist with include:

- Identify goals, pinpoint areas for growth, and create a plan for success.
- Understand security specialist core, supervisory and technical competencies.
- Discover training and professional development opportunities to build skills and maximize potential.

The ISC RMP Standard includes three FOUO appendices, Appendix A: The Design-Basis Threat Report (DBT), Appendix B: Countermeasures, and Appendix C: Child-Care Centers Level of Protection Template. To request access, e-mail ISCAccess@hq.dhs.gov.

2022 Edition: Appendix A: The Design-Basis Threat Report: Reviewed by the DBT Subcommittee and updated annually, this appendix establishes a profile of the types, composition, capabilities of adversaries, and characteristics of the threat environment to be used in conjunction with all ISC physical security standards. This year, the ISC DBT Subcommittee, in collaboration with the Argonne National Laboratory, updated the risk-utility model to determine baseline threat ratings. Significant updates include:

- 11 UE baseline ratings were increased.
- 12 UE baseline ratings were decreased.
- Updated executive overview of threats to federal facilities portraying relative threats between UE categories and individual UEs.

Keep a watch for the DBT Report data call for the 2023 edition. Department and agency responses are crucial to ensure the DBT is a comprehensive and credible report with representation from across the entire federal landscape. We are interested in incident data on facilities not covered by FPS or unique incidents you feel should be highlighted in the report.

2022 Edition: Appendix B: Countermeasures: Countermeasures helps federal agencies determine how to mitigate threats to federal facilities nationwide commensurate with the risk posed to a specific facility. It ensures the use of a comprehensive approach to meeting federal facility security needs in today’s threat environment. Key to this year’s update by the Countermeasures Subcommittee was a revision in the documents format. The Security Criteria tables have been substantially modified from previous versions. All information pertaining to each security criterion is now presented 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 CCC baseline LOP identified in Appendix C is now annotated in the security criteria tables.
- Highlights that the baseline level of protection is only applicable until a risk assessment can be performed.
- Emphasizes that risk acceptance can only occur after alternative risk mitigation strategies have been considered and documented.

Looking ahead to 2023, the ISC subcommittees and working groups are actively pursuing publication of several documents including *Making a Business Case for Security, An ISC Best Practice* and *Mobile Federal Workplace Security, An ISC Best Practice*. Two new working groups are projected to be started with a charter to update the ISC Guides on *Occupant Emergency Programs* and *Facility Security Plans*. If interested in participating on either of those working groups, stay alert for the recruitment emails.
For any questions about subcommittees or working groups, contact ISC.DHS.GOV@HQ.DHS.GOV.

Introducing Title 41, Part 102-81: FMR; Physical Security

By ISC Staff

Title 41, Part 102-81: 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 GSA, must comply with the policies and recommendations set by the ISC, this includes the RMP Standard.

effective 09.23.22

Title 41: Federal Management Regulation, Physical Security

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

Through this regulation, the GSA has further codified the ISC's RMP Standard as the benchmark to define the criteria and processes for determination of the facility security level (FSL) and to provide a single source of physical security countermeasures for nonmilitary Federal facilities. *Title 41 Part 102-81* states that, under Executive Order 12977, the ISC is the sole entity responsible for setting policies and recommendations governing physical security at nonmilitary Federal facilities and buildings under the jurisdiction, custody, or control of GSA. The goal of the RMP Standard is a level of protection commensurate with the level of risk. This update also calls out the role of departments and agencies in implementing, maintaining, and upgrading physical security standards and the role of Facility Security Committees (FSC), and the commitment of each occupant agency.

Other notable references include:

- The security organization responsible for the Federal facility or Federal grounds will conduct a periodic risk assessment and recommend countermeasures and design features to be implemented at the Federal facility.
- The FSC will determine whether the recommended countermeasures will be implemented, or risk accepted.
- Countermeasures, once approved, will require each Federal occupant in the building to be responsible for funding its *pro rata* share of the cost.
- GSA will assist with the implementation of approved countermeasures.

For more information on Title 41, *Part 102-81*, please visit the ISC's website: https://www.cisa.gov/isc

Welcome to the new ISC Regional Advisors

The ISC is pleased to announce that Mr. Brian Pavone and Mr. C. Kevin Choate have joined the ISC staff as new Regional Advisors. The ISC Regional Advisors serve as a resource to address ISC-related questions and concerns. They provide stakeholders at regional or field offices a variety of advisory services including outreach, training, and support for implementing compliance programs. Most of the Regional Advisor's efforts focus on raising awareness of ISC policies, standards, and recommendations, as well as the importance of reaching federal facility security compliance. Regional stakeholders include department and agency officials involved in federal facility security decisions, FSCs, Federal Executive Boards, security organizations, owning/leasing organizations, and Federal facility tenants.

Brian Pavone, Regional Advisor | Region 4

Brian Pavone comes to us from the Cybersecurity and Infrastructure Security Agency, where he was assigned as the Protective Security Advisor for the Northern District of Alabama.

Prior to joining CISA in October 2021, Brian served as the Deputy Branch Chief of Physical Security for the Centers for Disease Control and Prevention (CDC), responsible for field site physical security operations, guard force and electronic security system contract management, security engineering, protective intelligence, and threat management, as well as agency ISC compliance.

Before his work with the CDC, Brian worked for the Department of Defense (DoD) as the Mission Assurance and Critical Infrastructure Protection Section Chief at U.S. Southern Command; Director of Public Safety at Navy Region Center Singapore; and Critical Infrastructure Protection Analyst at U.S. Indo-Pacific Command. In addition, he briefly served a two-year stint as an Associate with Booz Allen Hamilton providing security consulting expertise to the DoD.

Preceding his work in the federal civil service and as a contractor, Brian served 24 years in the U.S. Navy, where he retired as a Security Limited Duty Officer (LT/O3E). Brian earned his Master of Arts degree in International Security Studies from the University of Arizona, and a Bachelor of Arts degree in Asian Studies from the University of Maryland University College.

Brian holds the following professional certifications: ASIS Certified Protection Professional (CPP), ALICE Certified Instructor (ACI) and NICP CPTED Professional Designation (CPD).

C. Kevin Choate, Regional Advisor | Region 6 & 8

Kevin Choate is a Security SME specializing in DoD and Executive Branch security risk management for more than 26 years. He joins the ISC having previously served in the DoD United States Air Force (USAF) Military Satellite Communication (MILSATCOM) where he supervised a $40 billion space portfolio as their Chief of Security. Most recently, Kevin was employed at the GSA Office of Mission Assurance in Region 10, which is the Pacific Northwest and Arctic jurisdictions.

In his role in GSA Region 10, Kevin frequently partnered with Federal Executive Boards, Regional Commissioners, Regional Agency Heads, and the Designated Officials/FSC Chairs as a security and ISC RMP SME.

ISCRMP & FSCTraining

The ISC, which addresses security for all federal facilities, has 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 & FSC Training is Instructor-led, provided by certified ISC Staff, to include ISC Regional Advisors – field personnel who provide outreach and capacity building to the 90% 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.

This training has been accredited by the International Accreditors for Continuing Education and Training (IACET) and awards Continuing Education Units (CEU). The training is offered at no cost to participants.

To request or schedule an in-person training, please send an email to RMP_FSCtrng@cisa.dhs.gov for more information: (in-person training dates are on a first come first serve basis).

2023 RMP & FSC Training Dates: In-Person

- April 27, 2023: Duluth, MN

For the list of virtual training dates visit the ISC website at: Interagency Security Committee Training | CISA

ISC Contact Information

ISC General Inquiries:

ISC.DHS.GOV@HQ.DHS.GOV

ISC Website:

https://www.cisa.gov/isc

Compliance Inquiries:

isccs-support@hq.dhs.gov

ISC Regional Advisors:

https://www.cisa.gov/isc-regional-advisors

Training Inquiries:

RMP_FSCTRNG@cisa.dhs.gov