ISC Quarterly Newsletter

December 22, 2023

Issue 30

Message from the Chair

ISSUE HIGHLIGHTS:

- Message from the Chair
- Executive Order 14111
- Introduction to TRIPwire
- An Overview of the ISC's Guidance Documents
- Facility Level Compliance
- New Team Member Highlight: David Hooker
- 2023 ASTOR Awards

As we conclude 2023, I reflect on the great work the ISC has completed and point a light at the impetus President Biden's signing of Executive Order 14111 will bring. Since the bombing of the Alfred P. Murrah Federal Building in Oklahoma City twenty-eight years ago, our committee has achieved significant progress and made tremendous strides in enhancing the security and protection of federal facilities. Congratulations on a new executive order and the new responsibilities and authorities it will bring.

It was wonderful to have so many participate in the fall ISC Membership Meeting on Tuesday September 19, 2023. I would like to thank the Internal Revenue Service (IRS) for hosting an informative, productive meeting that led to numerous insightful and enlightening conversations. My sincere appreciation to the IRS for their valuable presentation on their Facility Risk and Priority Register, and to the General Services Administration (GSA) for providing an overview on the recently published Mail Center Security Guide. This document represents a great partnership between the ISC and GSA in creating this comprehensive resource.

I am also pleased to announce the ISC's successful migration to TRIPwire to house all "For Official Use Only (FOUO)" publications. The transition to this new platform will result in a user-friendly access format to locate and retrieve pertinent federal facility security resources.

Finally, I would like to highlight the dedicated work of the ISC Subcommittees to produce two updated appendices to the Risk Management Process (RMP) Standard; Appendix A: Design-Basis Threat (DBT) Report, and Appendix B: Countermeasures. Both appendices are vital to the protection of federal facilities as well as their workers and visitors.

Lastly, as we embark upon the holiday season, I wish you a very happy, relaxing, and safe holiday with your family and friends. I am proud to stand alongside each of you as we continue to advance the mission of the ISC, and I look forward to the many meaningful projects to come in the new year.

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

2024 ISC Membership Meetings

The next ISC Membership Meeting will be held on March 19, 2024. More information coming soon!

2024 ISC Trainings

Visit the ISC's Training page for updated information on upcoming training opportunities.

Executive Order 14111 Reinforces President's Commitment to Federal Facility Security

By ISC Staff

Caitlin Durkovich, National Security Council, The White House, at the EO Signature Celebration Ceremony on November 27, 2023

President Biden signed Executive Order 14111, which is intended 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 Executive Order 14111, a Signature Celebration Ceremony was held on November 27, 2023, at the Eisenhower Executive Office Building.

The signing of Executive Order (EO) 12977 on October 19, 1995 created the Interagency Security Committee (ISC). Following the bombing of the Alfred P. Murrah Federal Building in Oklahoma City, the ISC was established to enhance the security and protection of federal facilities.

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

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

The following are the major updates in 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 facility security committees.
- Established minimum compliance monitoring requirements for the Department of Homeland Security, to include conducting risk-based compliance verification.
- Updated the definition of federal facilities to reduce ambiguity.

Nitin Natarajan, Deputy Director, Cybersecurity and Infrastructure Security Agency, at the EO Signature Celebration Ceremony on November 27, 2023

The ISC would like to acknowledge and thank the Administration and members of the NSC for their leadership, dedication, and persistence to keep federal facility security a national priority.

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

ISC Document Migration: From HSIN to TRIPwire

By ISC Staff

Information is power that is constantly changing. Finding order amid chaos is essential. Sound knowledge management practices work to reduce the maze of resources and documents dispersed over multiple locations. Over the last year, the Interagency Security Committee staff studied multiple options for improving the ISC's repository of standards and policies and selected an improved solution to migrate the documents and resources from various locations into a singular, cohesive repository.

Stakeholders seeking to access the ISC's current publications, legacy documents, and FOUO documents have customarily used the Homeland Security Information Network (HSIN). As of October 4, 2023, ISC documents are available and accessible through CISA's Office of Bombing and Prevention's (OBP) TRIPwire website, which eases the process of locating and accessing documents and supporting material. The ISC Portal on TRIPwire organizes documents by category, such as Standards and Policies, Best Practices, Guidance Documents, and White Papers.

Co-located with these core documents and best practices are associated documents that harness their supporting relationship with the Risk Management Process (RMP). The new layout aligns each of these supporting resources with the RMP's base documents. If you are currently a member of the ISC community of interest on HSIN, you should have received an email informing you of the migration and how to register for access to the ISC Portal on TRIPwire.

To register for the ISC Portal on TRIPwire, go to https://tripwire.dhs.gov or contact the ISC at ISCAccess. Should you have any questions, please contact the ISC staff at ISC.DHS.GOV@HQ.DHS.GOV.

ISC Risk Management Process Standard and Its Associated Documents

By: ISC Staff

The ISC RMP Standard is the foundational doctrine for managing security risk for federal facilities. We all know the RMP has key appendices, such as the Design-Basis Threat (DBT) Report to support the RMP, but did you know the ISC has published numerous supporting documents through the Best Practices Subcommittee? These documents support the RMP and are now conveniently located together on TRIPwire.

Some other supporting resources include:

- A Facility Security Committee (FSC) Compliance Tracker. It provides a mechanism for FSCs to track and verify their adherence to security protocols, promoting transparency and accountability. This tracker ensures the effective implementation, measurable success, and maintenance of security measures, in compliance with the RMP Standard.
- The ISC's Best Practices for Lock and Key Control. This document supports Appendix B: Countermeasures of the RMP in helping to create a proactive and layered approach to physical security. This methodology offers specific recommendations and guidelines for securing access points, managing keys, and safeguarding sensitive areas.
- "Protecting Against Violent Civil Disturbance." The supporting resource offers guidance to federal agencies on preparing for and responding to increasing violent activities that pose significant security threats.

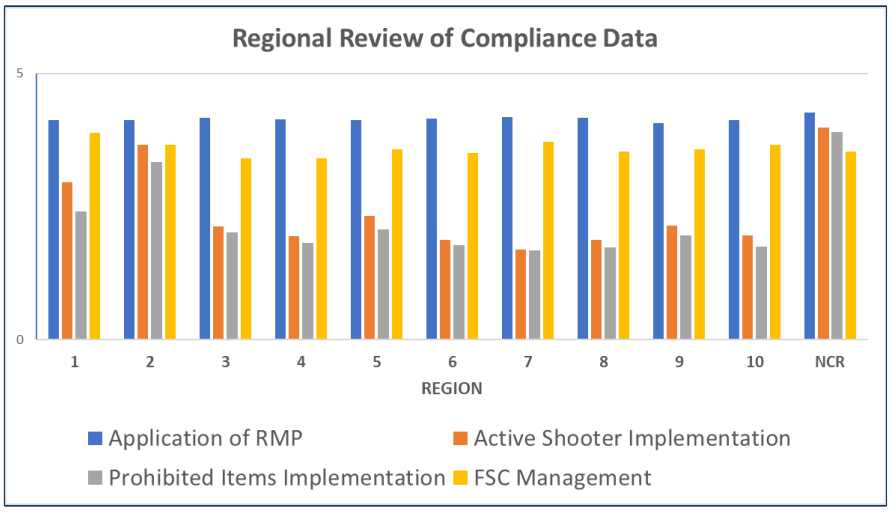
Facility Level Compliance

By: ISC Regional Advisor, CISA Regions 9 and 10

Compliance reporting provides ISC members with the means to measure, report, and analyze compliance with ISC policy and standards. As we continue to progress with compliance verification and to ensure facilities across the nation are protected as intended by Executive Order 14111, all members and security decision makers should consider further incorporating the ISC's policy and standards at the facility level.

As shown in the chart below, there are varying levels of implementation for the core ISC standards and policy across the regions. There is still work to be done with regard to implementing active shooter preparedness plans and the Prohibited Items Standard. Beyond self-reporting and verification of compliance information, the ISC's Regional Advisors (RAs) are available to assist with increasing compliance with ISC policy and standards at the facility level. ISC RAs can provide guidance and technical assistance through plan review and development, as well as exercise planning, seminars, and workshops. Your Regional Advisor's contact information can be found at this link: Interagency Security Committee Regional Advisors | CISA.

To stay informed on regional information from your RA, you are encouraged to join your regional distribution list by signing up at this link: ISC Regional Distribution List.



New Team Member Spotlight: David Hooker

By: ISC Staff

David Hooker joined the ISC in September 2023 and comes to us from a diverse background in program management and military service. His prior work supported the Department of the Navy in program management and acquisition within the Navy Enterprise Resource Planning Program, Strategic Systems Program, Virginia Class New Construction Program, as well as Naval Information Warfare Systems Command.

Prior to his support through the defense contracting workforce, David served as a Surface Warfare Officer in the U.S. Navy. While serving, his notable efforts included supporting CENTCOMs crisis response force through leading regional security planning and coordination of contingency assets and personnel throughout the Middle East. He also led the effective employment of weapon systems on the USS Boone and strategic planning for Amphibious Squadron 11 in Sasebo, Japan.

David is married with two children and resides within Virginia. He graduated from Vanderbilt University in 2008 with a Bachelor of Science in Engineering Management and a minor in Systems Engineering.

ISC and Design-Basis Threat Subcommittee Win Platinum 'ASTORS' Homeland Security Awards

By: ISC Staff

2023 'ASTORS' Homeland Security Award for Excellence in Public Safety

For the third consecutive year, the ISC's Risk Management Process and Facility Security Committee Training (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.

2023 'ASTORS' Homeland Security Award for Excellence in Federal Government Security Program

The Design-basis Threat (DBT) Subcommittee, in partnership with the Federal Protective Service (FPS) and Argonne National Lab (ANL) won the 2023 'ASTORS' Homeland Security Award for Excellence in Federal Government Security Program for development of an updated threat analysis methodology. This 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 into a three-objective model that includes capability, history, and intentions, allowing for further depth of analysis and comparison of threats to federal facilities.

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