An Introduction to the Interagency Security Committee
2013
The Creation of the ISC

• April 19, 1995: Oklahoma City Bombing
  – The day after the bombing, President Clinton realized Federal buildings were vulnerable to attack and no minimum security standards in place.
  – Directed the Department of Justice to assess the vulnerability of Federal Facilities to acts of terrorism and violence, and to develop recommendations for minimum standards.

• June 28, 1995: Department of Justice issued the Landmark *Vulnerability Assessment of Federal Facilities Report*
  – Created 52 minimum security standards; and
  – Recommended establishing an Interagency Security Committee (ISC).
On October 19, 1995 President Clinton Signed Executive Order 12977

• **Duties and Responsibilities:**
  – Establish policies for the protection of non-military Federal facilities;
  – Develop and evaluate security standards; and
  – Take such actions as may be necessary to enhance the quality and effectiveness of security of Federal facilities.

• “It will provide a permanent body to address continuing government-wide security for Federal facilities,” and

• “Each executive agency and department shall cooperate and comply with the policies and recommendations of the Committee issued pursuant to this order.”
On October 19, 1995 President Clinton Signed Executive Order 12977, continued

- **Additional Duties and Responsibilities:**
  - Encourage agencies to share security related intelligence
  - Assess technology/Information
  - Develop long-term construction standards
  - Evaluate standards for special security situations
  - Assist in developing and maintaining a centralized security database of all Federal facilities

- The creation of the ISC marked the beginning of collaboration and communication across Federal agencies’ security personnel and senior executives. For over 15 years they have worked together to create Federal facility standards and guidelines.
ISC Governance Today

Chairman
Assistant Secretary for Infrastructure Protection

Executive Director
Operates the day to day activities.

Subcommittees - (Ongoing)
Identify priorities and oversee strategic initiatives.

• Steering – approve initiatives
• Standards – review initiatives
• Convergence – collaboration between Physical Security/ Information Technology
• Technology Best Practices – Evaluate technology solutions

• Training – oversee ISC training Initiatives
• Countermeasures – oversee the development of countermeasures
• Design-Basis Threat – establishes a profile of type, composition, and capabilities of our adversaries

Working Groups - (Task Specific)
ISC Members (53)

PRIMARY MEMBERS (21)

1. Assistant to the President for National Security Affairs
2. Central Intelligence Agency
3. Department of Agriculture
4. Department of Commerce
5. Department of Defense
6. Department of Education
7. Department of Energy
8. Department of Health and Human Services
9. Department of Homeland Security
10. Department of Housing and Urban Development
11. Department of the Interior
12. Department of Justice
13. Department of Labor
14. Department of State
15. Department of Transportation
16. Department of the Treasury
17. Department of Veterans Affairs
18. Environmental Protection Agency
19. General Services Administration
20. Office of Management and Budget
21. US Marshals Service

ASSOCIATE MEMBERS (32)

1. Commodity Futures Trading Commission
2. Court Services and Offender Supervision Agency
3. Federal Aviation Administration
4. Federal Bureau of Investigation
5. Federal Communications Commission
6. Federal Deposit Insurance Corporation
7. Federal Emergency Management Agency
8. Federal Protective Service
9. Federal Reserve Board
10. Federal Trade Commission
11. Government Accountability Office
12. Internal Revenue Service
13. National Aeronautics & Space Administration
14. National Archives & Records Administration
15. National Capital Planning Commission
16. National Institute of Building Sciences
17. National Institute of Standards & Technology
18. National Labor Relations Board
19. National Science Foundation
20. Nuclear Regulatory Commission
21. Office of the Director of International Intelligence
22. Office of Personnel Management
23. Office of the U.S. Trade Representative
24. Securities and Exchange Commission
25. Smithsonian Institution
26. Social Security Administration
27. U.S. Army Corps of Engineers
28. U.S. Capitol Police
29. U.S. Coast Guard
30. U.S. Courts
31. U.S. Institute of Peace
32. U.S. Postal Service
Importance of the ISC

- A truly interagency body exhibiting collaboration and communication between 53 Federal agencies and departments;
- When agencies cannot solve security related problems on their own, the ISC brings chief security officers and senior executives together to solve continuing government-wide security concerns;
- Responsible for the creation and implementation of standards, guidelines, and best practices for the protection of over 300,000 nonmilitary Federal facilities across the country;
- The work is based on real-world, present-day conditions and challenges; and
- Cost savings by focusing on specific security needs of the agencies.
How the ISC Works

Interagency Security Committee Working Group Process Map

1. Sponsor
   - Sponsoring Idea
   - Create Issue Paper
   - Steering Review via Executive Director

2. CIISC
   - Discuss with Executive Director
   - Chair Approves/Declines New Product
   - Create Charter

3. Sub-Committees
   - 8 Working Group Formed
   - 9 Notice to Proceed Issued
   - 10 Meets to Complete Objective
   - 11 Standards SC Review
   - 12 Chair Briefed on Draft
   - 13 Full Membership for 30-Day Comment
   - 14 Members Comments Compiled for Review
   - 15 Comments Reconciled Creating Record
   - 16 Creates Final Draft
   - 17 Primary Membership for Day Vote
   - 18 Steering Review of Vote (if necessary)
   - 19 Review & Closeout
   - 20 Final Edit & Legal Review
   - 21 Chair Final Approval & Signature
   - 22 Final Published
Risk Management Process Documents

1. (FOUO) Facility Security Level Determinations for Federal Facilities Standard
5. Use of Physical Security Performance Measures
7. Standard Operating Procedures for Risk Assessment Data Tool Validation
Facility Related Documents

9. Occupant Emergency Programs: An ISC Guideline
10. Best Practices for Working with Lessors (Comment Period)
11. (FOUO) Best Practices for Mail Screening and Handling
13. Items Prohibited from Federal Facilities: An ISC Standard
Personnel Related Documents

Training
17. ISC Training Programs
18. Standard Operating Procedures for Certifying Training Courses/Programs

Newsletters, White Papers and New Initiatives
21. Lessons Learned/Best Practices Work Group Newsletters (Continuous)
22. Technology Best Practices Subcommittee Newsletters (Continuous)
Risk Management Process Documents

- Combines five fundamental ISC documents into one document:
  1. (FOUO) Facility Security Level Determinations for Federal Facilities Standard
  5. Use of Physical Security Performance Measures

- The ISC Risk Management Process
  1. Determine the Facility Security Level (FSL);
  2. Identify baseline level of protection (LOP);
  3. Identify and assess the risks;
  4. Determine the required or highest achievable LOP; and
  5. Implement countermeasures.
Standard Operating Procedures for Risk Assessment Data Tool Validation

• First step towards soft compliance;
• Strategy for Federal departments and agencies to ensure their risk assessment data tool is compliant with ISC standards;
• Defines the necessary and/or actions that must be taken for risk assessment data tools to be validated as compliant with the ISC Standards.

- Updates government-wide guidance for prevention and response.
- Provides case studies as examples of the types of incidents reported.
- Representatives of DHS, DOI, VA, OPM, and FDIC serve on the working group.
Occupant Emergency Program: An ISC Guideline

- Defines the basic guidelines/procedures agencies may use when developing and implementing an Occupant Emergency Plan.
- Representatives of DHS, State, GSA, DOC, DOL, EPA, FEMA, FBI, FAA, ODNI, OPM, USPTO, USCIS, and NIST serve on the working group.
Items Prohibited from Federal Facilities: An ISC Standard

• Fills the void for a government-wide baseline list of items prohibited from entry into all nonmilitary Federal facilities to ensure consistency and prevent confusion and outlines a process for granting exceptions

• Prohibited items may include dangerous, unlawful, or otherwise determined to create vulnerabilities to the tenant agency(s)

• Working group: DOE, DOI, DOL, GSA, FPS, US Courts, and PFPA on the.
Best Practices for Federal Mobile Workplace Security (Development Period)

• The primary mission is to analyze the future impact on physical and cyber security policy and practices (telecommuting centers and hotel-type workplaces).

• Survey current body of knowledge, identify gaps, and present recommendations.

• Recommend appropriate roles and responsibilities for employees, supervisors, and security providers.

• Representatives of S&T/DHS, USDOJ, FAA, FPS, DOE, USCIS, USMS, FTC, serve on the working group.
• Will assist Federal government tenants, security organizations, and leasing staff when working with lessors to implement appropriate security countermeasures.

• The document will cover procedures/protocols for:
  – Key player responsibilities; and
  – Pre-Award and Post Award meetings.

• Representatives of DHS, DOJ, DOD PFPA, DOL, GSA, FPS, USMS, and FAA serve on the working group.
(FOUO) Best Practices for Mail Screening and Handling

- Provides mail center managers with a framework for understanding and mitigating risks posed to an organization by the mail and packages it receives and processes on a daily basis.
- First time a document written largely by another Federal government entity.
- Developed by the Department of Defense, Combating Terrorism Technology Support Office (CTTSSO), Technical Support Working Group (TSWG); and the ISC.
At the request of leadership, a non-FOUO version of the FOUO Mail Screening and Handling document was requested to be made available to the private/commercial sectors.
Personnel Related Documents
For the first time, establishes a government-wide baseline set of best practices to be applied to all Armed Security Officers working at nonmilitary Federal facilities in the United States.

The document covers:
- Citizenship; Experience;
- Equipment; Uniforms; Grooming;
- Medical & Physical Standards; and Training.

Representatives of DHS, CIA, DOJ, DOT, DOEd, IRS, EPA, FPS, FAA, SSA, and FDIC serve on the working group.
Security Specialist Competencies: An ISC Guideline

• Provides the range of core competencies for Security Specialists, to include:
  – Security and Emergency Policies;
  – Facility Security Assessments;
  – Information, Communication, Personnel Security;
  – Incident Management and Continuity of Operations;
  – Security Countermeasures; and
  – Contracting.

• Does not cover unique requirements of individual Federal departments and agencies or for certain specialized positions.
Training
ISC Training Programs

Web Based

- IS-890 Introduction to the ISC
- (FOUO) IS-891 Facility Security Level Determination for Federal Facilities
- (FOUO) IS-892 Physical Security Criteria for Federal Facilities
- IS-893 Facility Security Committees in Federal Facilities

Classroom

- Three Day - Risk Management Process Training Course (DOJ/GSA/DHS)
Standard Operating Procedures for the Certification of Training Courses & Programs

• Establishes the baseline criteria and/or actions that must be taken for certifying training courses and programs as compliant with the Interagency Security Committee (ISC) published Standards and guidelines.
Newsletters, White Paper, and New Initiatives
Convergence Subcommittee
White Paper (Development Period)

• Recommendations will provide traditional security and IT professionals with mechanisms to support security programs, while integrating information assurance management controls.
Lessons Learned/Best Practices
Working Group Newsletter

• Establishes an interagency information sharing forum.
• Developed a newsletter to deliver lessons learned for members.
• Representatives of IRS, USMS, FBI, DHS, DOT, DOI, DOE, FPS serve on the working group.
Technology Best Practices
Subcommittee Newsletters

• Provides a newsletter on the efficient uses of technology that supplement and reinforce other security measures in cost-effective ways.
New Initiatives

1. **Facility Security Plan WG** - utilize the ISC’s Risk Management Process to develop guidance agencies can use to formulate a Facility Security Plan.

2. **Security Office Staffing WG** - establish criteria and policies which will inform agencies staffing of a Security Office.

3. **Resource Management WG** - develop guidance to help agencies make the most effective use of resources.

4. **Presidential Policy Directive 21 and Compliance WG** – develop security criteria for critical infrastructure supporting mission essential functions to account for PPD21 requirements and to create a strategy for compliance.

5. **Active Shooter WG** - will focus on developing a single cohesive document with greater concentration on Active Shooter.
More About the ISC

• To request access to ISC FOUO documents and training: ISCAccess@dhs.gov

• Website: www.dhs.gov/isc