



# Interagency Security Committee

## *Smart Security in Federal Buildings*



Homeland  
Security

Bernard Holt  
Interagency Security Committee  
Office of Infrastructure Protection  
November 4, 2010



# An Introduction to the ISC

- The Interagency Security Committee (ISC) is dedicated to the protection of civilian Federal facilities in the United States.
- **Mission:** We safeguard U.S. civilian facilities from all hazards by developing state-of-the-art security standards in collaboration with public and private homeland security partners.
- Today the ISC works to ensure security for:
  - **1.2 million** federally owned and leased facilities
  - **2.5 million** civilian workers and over 8,000 children in child-care centers
  - **3.26 billion** square feet of property with a replacement value of \$371 billion

*(Source: Key Statistics: FY2008 CFO Act Agencies, Federal Real Property Report, Federal Real Property Council & American History Magazine)*
- President Clinton issued Executive Order 12977 creating the ISC soon after the Oklahoma City bombing on April 19, 1995.



# The Bombing of the Alfred P. Murrah Federal Building



**It was the deadliest terrorist attack on U.S. soil before 9/11. It is still the worst domestic-based terrorist attack in U.S. history.**



# History of the Development of American Federal Security Policy

- **Soon after the Oklahoma City bombing, the U.S. Department of Justice (DOJ) conducted a *Vulnerability Assessment Study* – issued on June 28, 1995. It:**
  - Created 52 minimum security standards
    - based on a building's assessed security level: Level I – V
  - Also recommended creation of an Interagency Security Committee (ISC)
- **Prior to 1995:**
  - No minimum physical security standards for non-military federally owned or leased facilities existed
  - There was no Federal authority to assess vulnerability, develop security standards and policies, or oversee compliance for non-military Federal facilities



# ISC Governance

- The ISC is a component of (DHS), National Protection and Programs Directorate (NPPD)
- The Chair of the ISC is the DHS Assistant Secretary for Infrastructure Protection (IP), Mr. Todd Keil
- The ISC members meet quarterly
- The following subcommittees guide/direct the work of the ISC
  - **Steering Subcommittee** – Provides input on priorities; proposed initiatives/projects
  - **Standards Subcommittee** – The focal point for coordination of all ISC standards
  - **Technology Best Practices Subcommittee** – Identifies practices in cutting-edge security technology and guidance on cost-effective use of new technology to supplement and reinforce other security measures
  - **Convergence Subcommittee** – Provides subject-matter expertise on best practices in providing agencies with mechanisms to support security programs, while integrating information management controls through a collaborative effort



# Over 120 Senior Executives From 47 Federal Agencies and Departments Comprise the ISC

## Primary Members represent 21 Federal agencies

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 represent 26 additional agencies

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



# The ISC: Working Together

- **The ISC provides coordinated interagency solutions to problems which cannot be solved by individual departments and agencies alone.**
- **Strong participation of ISC members in subcommittees and working groups.**



**ISC members discuss recommendations at a Quarterly Meeting.**



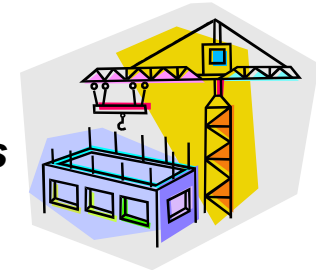
# The ISC Approach from 1995-2009

- Physical security within the ISC portfolio was governed by three standards documents:

- 1995 DOJ Vulnerability Assessment of Federal Facilities



- 2004 ISC New Construction Criteria for Federal Facilities



- 2005 ISC Leased Facilities Criteria for Federal Facilities





# The ISC Approach from 1995-2009

(cont.)

## Why update the DOJ Report and ISC Standards Now?

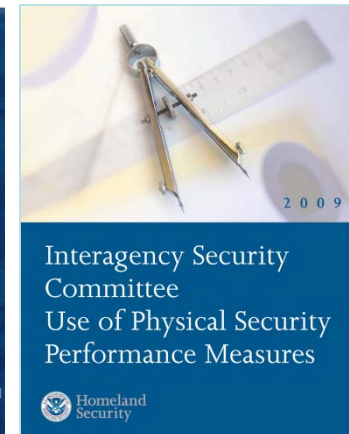
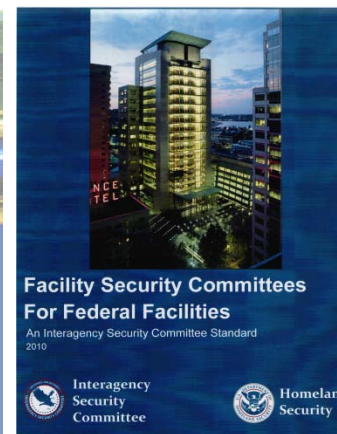
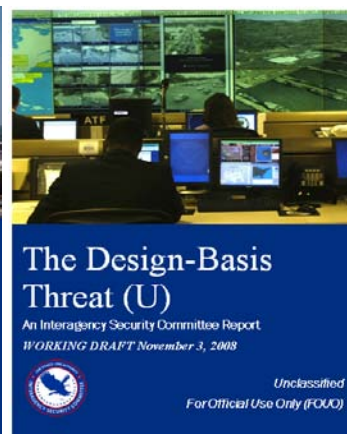
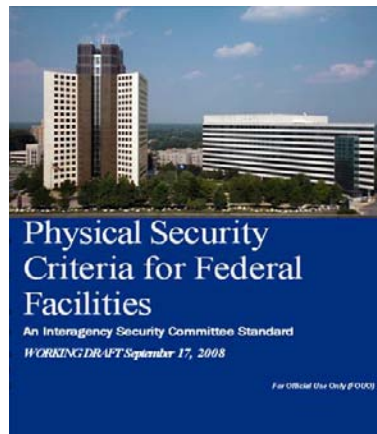
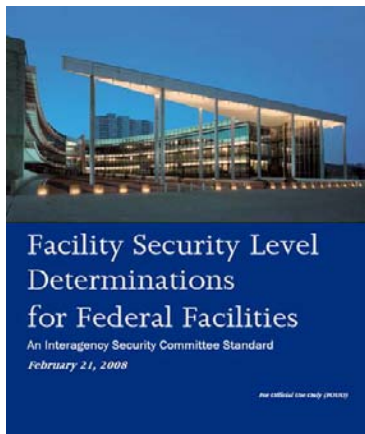
- DOJ report was 15 years old, inconsistent application
- Inconsistencies between the different levels of protection for leased buildings vs. owned & design basis threat & the use of multiple documents
- New construction not tied to facility security levels
- *Competition in Contracting Act* may prohibit using two different standards for the same acquisition
- Advances in technology
- No waivers



# The ISC Approach 2010

## Smart Security in Practice

Addresses the full-spectrum of security threats & current and future risks & replace the 1995 DOJ Report and 2004 New Construction and 2005 Leased Facilities Criteria for Federal Facilities





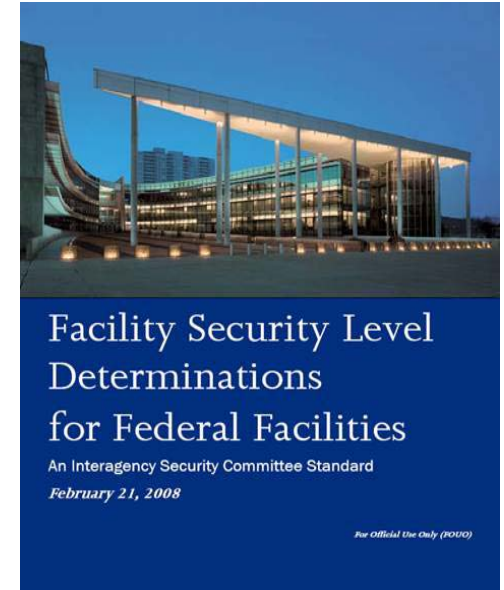
# Key Components of the ISC Standards

- **One formalized process to:**
  - Determine risks
  - Identify desired level of protection
  - Identify when the desired level of protection is not achievable
  - Develop alternatives
  - Accept risk when necessary
- **Creates the concept of a common threat truly “risk based” concept:**
  - Identical risks will be handled in an identical manner
- **Provides and ensures:**
  - Equivalent mitigation strategies for equivalent risks
  - Customized templates for agencies with repetitive requirements (Child-Care, Courthouses)
- **Risk acceptance:**
  - Do less or do nothing are **valid alternatives** if full mitigation of risk is not possible



# Facility Security Level (FSL) Determinations for Federal Facilities 2008

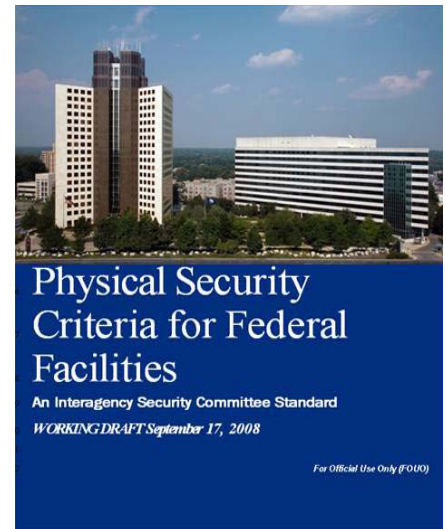
- **Foundation for the ISC Risk Management Process which defines the criteria and processes a facility should use to determine its FSL which serves as the basis for implementing measures under other ISC Standards.**
- **The FSL is the result of an assessment that assigns each facility a level from I-V based on the criteria below:**
  - Size
  - Symbolism
  - Population
  - Threat to tenant agency
  - Mission criticality





# New 2010: *Physical Security Criteria (PSC) for Federal Facilities*

- The culmination of three year effort by the ISC.
- Establishes a baseline of the specific countermeasures to be implemented for each facility security level. It further provides a framework for the customization of security measures to address unique risks at each facility
- It updates and combines other ISC Standards bringing together criteria for existing, owned, leased, and new construction for Federal facilities, and offers more flexibility and provides:
  - An integrated, single source of physical security standards
  - Single source of countermeasures for each security level
  - Produces a baseline for measurement
  - Increase usability and understanding
  - Leverages the latest technology
  - Assure formalized acceptance of risk and accountability





# Customization Options in the PSC Enable Smart Security Solutions (cont.)

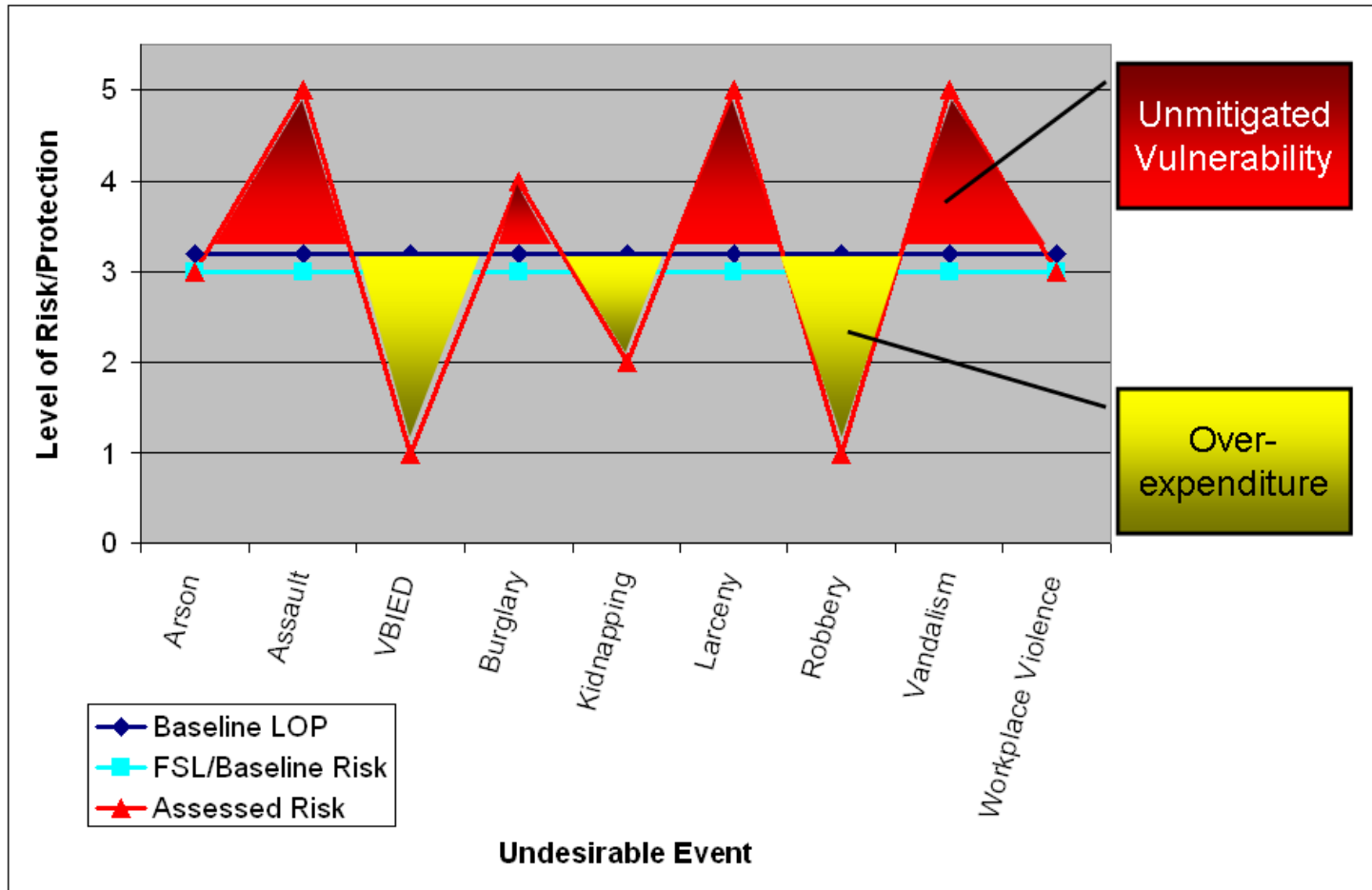
- **The decision making process contained in the PSC allows the following results:**
  - The application of a baseline Level Of Protection (LOP) applicable to the facility's Facility Security Level (FSL)

**OR**

  - The application of a customized Level of Protection to address facility-specific conditions when the acceptance of risk may be unavoidable due to factors such as, but not limited to, the following:
    - Mission requirements
    - Physical site limitations
    - Historical/Architectural integrity
    - Funding Priorities
- **This allowance for customization provides flexibility within the common framework of the Physical Security Criteria Standard.**

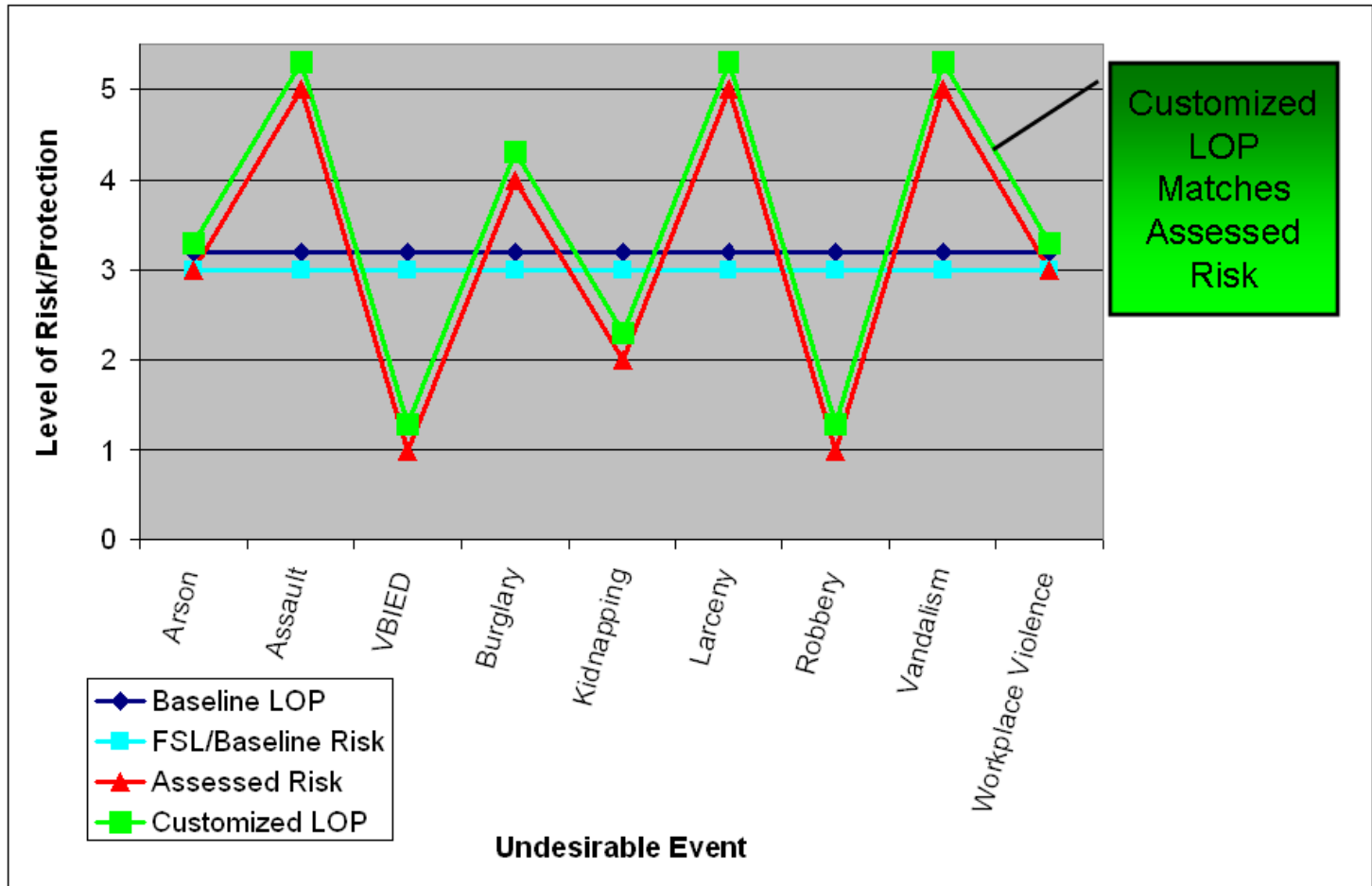


# With the Old Standard (PSC cont.)





# With the New Standard (PSC cont.)

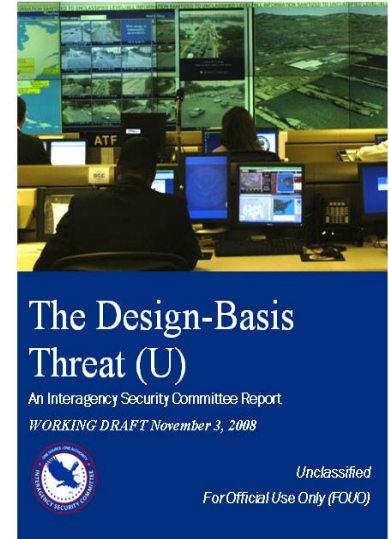




# New 2010: *Design-Basis Threat (DBT) Report* (First-of-its-kind report)

- **Purpose:**

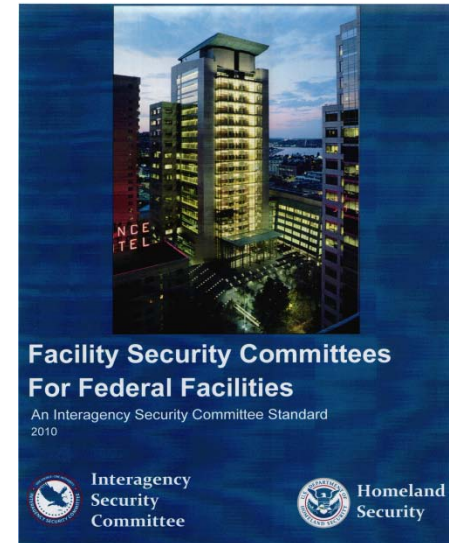
- Identifies the baseline threat to Federal facilities when applying the ISC PSC Risk Management Process
- Supports the calculation of risk - based upon threat, vulnerability, and consequences to a facility when applying the ISC's PSC
- Fills the void of threat information available to security managers
- Determine specific adversary characteristics that performance standards and countermeasures are designed to overcome





# Facility Security Committee Standard (coming late 2010)

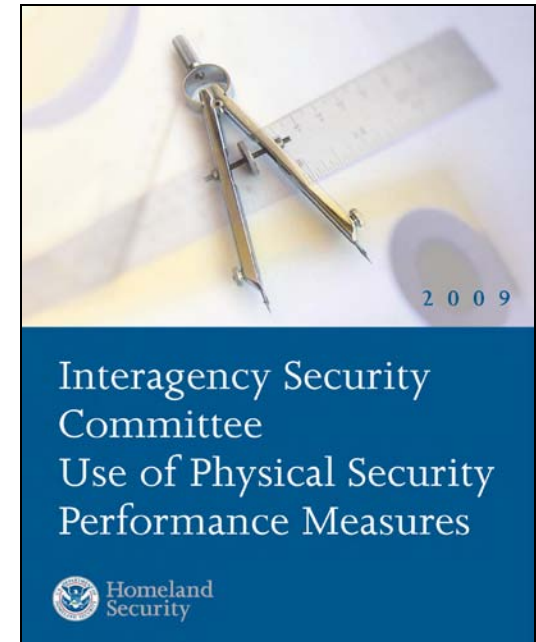
- Previously known as Building Security Committees (BSCs)
- Were established in 1995 by guidance provided in the DOJ Report with minimal guidance for their operation
- Defines the composition, responsibilities and roles of FSC members
- Establishes procedures to guide for FSC's through decision making, risk acceptance, and the documentation requirements





# *Use of Physical Security Performance Measures 2009*

- **First of its kind guidance created in response to a recommendation from the U.S. Government Accountability Office (GAO)**
- **Provides guidance on metrics and testing to evaluate physical security programs**
- **Necessary to show a security program's capabilities and effectiveness**
- **Both a Standard and a Best Practice**
  - Requires all ISC members to have a performance measurement program
  - Outlines best practices for doing so





# The ISC Risk Management Process





# Other 2010 Initiatives

- ***Minimum Standards for Armed Security Officers:***
  - Defines a baseline and set of minimum standards for determining the duties and responsibilities of a contract security force in all Federal facilities used for nonmilitary activities
- ***Security Specialist Competencies Guidelines:***
  - Details the core competencies federal security specialists should have to perform their basic duties and responsibilities
- ***Prevention of Workplace Violence Guidelines:***
  - Developed with Chief Human Capital Officers (CHCO) Council and the National Institutes of Occupational Safety and Health (NIOSH)
- ***Nationwide Training:***
  - Introduces the Compendium of Standards



# ISC Training to Support Implementation of **New** Standards

## List of Courses

COURSE	WEB - BASED	CLASSROOM	ATTENDEES
<b>IS-890: Introduction to the ISC (Private Sector)</b>	1 hour	2 to 3 hours	Federal Employees and anyone interested in the ISC
<b>IS-891: Facility Security Level (FSL) Determinations (FOUO)</b>	1 hour	2 hours	Law enforcement, FSC Members, and Physical Security Specialists
<b>IS-893: The Physical Security Criteria Processes (FOUO)</b>	2 hours	1 or 2 Days	Law enforcement, FSC Members, and Physical Security Specialists
<b>IS-894: Private Sector Overview of the ISC Processes (Private Sector)</b>	1 hour	2 to 3 hours	Building Owners, Developers, Architects, Law enforcement, Security Professionals, and others
<b>IS-895: Facility Security Committee (FSC) Process (FOUO)</b>	1 hour	2 to 3 hours	Law enforcement, FSC Members, and Physical Security Specialists



## Interagency Security Committee

# Looking for more information?

- **Website:** [www.dhs.gov/isc](http://www.dhs.gov/isc)
- **Email:** [ISC@DHS.GOV](mailto:ISC@DHS.GOV)
- **ISC Standards Documents and products**
  - Currently *For Official Use Only* (FOUO) – is limited to U.S. government users
  - Access to the ISC Document Library (hosted on Homeland Security Information Network HSIN) is limited to U.S. government users



Homeland  
Security



**Interagency  
Security  
Committee**

# Questions?

**Austin Smith**

**[Austin.Smith@dhs.gov](mailto:Austin.Smith@dhs.gov)**

**703.603.5128**

**Bernard Holt**

**[Bernard.Holt@dhs.gov](mailto:Bernard.Holt@dhs.gov)**

**703.603.5165**



**Homeland  
Security**