Security Specialist Competencies:
An Interagency Security Committee Guide

January 2017
2nd Edition

Interagency
Security
Committee

Change History and Document Control

Rev. #	Date	Changes	Approver
1.0	01/2012	Initial Issue	ISC
2.0	01/2017	Competencies Updated/Cyber Category Added	ISC

Message from the Program Director

As Program Director of the Interagency Security Committee (ISC), I am pleased to introduce the 2nd edition of *Security Specialist Competencies: An Interagency Security Committee Guide*. The guide provides the range of core competencies Federal security specialists should possess to perform their basic duties and responsibilities.

One of our top national priorities is the protection of all Federal employees and occupants who work within and visit Federal government-owned or leased facilities. Composed of 60 Federal departments and agencies, the ISC's primary mission is to craft security standards and best practices for non-military Federal facilities in the United States.

The ISC's objective in creating this guide was to develop recommendations all Federal agencies could use to increase core competencies for security specialists. By establishing a common baseline of knowledge and abilities for training and professional development, security specialists in any given agency would be proficient to a unified, minimum capability.

This guide is a significant milestone and represents exemplary collaboration within the ISC working group, Training Subcommittee, and across the entire ISC. The ISC will review and update this guide as needed.

Daryle Hernandez
Program Director
Interagency Security Committee

Table of Contents

1.0 Background

Security specialists have historically played a key role in Federal facility protection and emergency planning efforts. However, security specialist qualifications have largely been determined at the individual agency level, resulting in wide-ranging skill sets across the interagency community and revealing a clear need for consistency in security personnel qualifications and training in today's threat environment. Therefore, based on the Government Accountability Office's recommendation to promote strategic management of human capital, the Interagency Security Committee (ISC) convened a working group to develop a recommended baseline level of skills, knowledge, abilities, and competencies that security specialists throughout the Federal Government should possess.

The working group's objective was to develop a baseline that all agencies could use to increase core competencies for security specialists. By establishing and implementing a common baseline of knowledge and abilities for training and professional development, all security specialists in any given agency would be proficient to a unified, minimum capability.

This guide was initially developed by compiling known core competencies into a baseline draft document which was distributed, reviewed, and voted on by the ISC membership consisting of expert security practitioners. Comments were then evaluated and integrated into the draft document forming a baseline of core competencies (as perceived by the membership). Originally published in 2012, this guide reflects the efforts of the original working group, as well as the subsequent effort to review and update the document by the Training Subcommittee.

2.0 Applicability and Scope

Pursuant to the authority provided to the ISC in Section 5 of Executive Order (E.O.) 12977, as amended by E.O. 13286, this ISC document provides guidance to Federal departments and agencies for use in developing educational and training initiatives to improve the competencies of security specialists in the Federal workforce. In addition to the competencies presented herein, security personnel may be required to be familiar with department or agency-specific policies and requirements.

This guide provides the range of core competencies that security specialists in the Federal workforce should possess to perform their basic duties and responsibilities. The work of security specialists may be very broad or narrow, covering a single functional area or several, and may concentrate on specific subject matter areas. Accordingly, security specialists may develop competencies that are concentrated in one or more functional areas. This guide does not cover unique requirements of individual Federal departments and agencies or additional training and certifications for specialized positions, such as a communications security (COMSEC) officer, information security officer, compliance/oversight officer, executive protection specialist, or others. The ISC recognizes Federal departments and agencies will implement this guidance in a manner that reflects the unique and varied mission requirements and capabilities of their respective components.

3.0 Methodology

This document presents a series of subject areas with corresponding security specialist competencies. These competencies represent a baseline for all security specialists as they progress toward reaching the full performance level in one or more of the security disciplines. Further, it must be noted that the competencies outlined in this document specify the baseline knowledge, skills, and abilities that security specialists should possess and that would require validation by an individual's supervisor, rather than a mandate for a specified number of course hours. A variety of activities may be used to achieve the desired competencies, including, but not limited to:

- Correspondence courses;
- Internships/apprenticeships;
- Mentoring;
- On-the-job training;
- Rotational assignments;
- Self-study;
- Shadowing;
- Special projects/assignments;
- Structured classroom/performance-based training; and/or
- Web-based instruction.

4.0 Security Specialist Competencies

The subject areas and competencies identified in this section outline the general knowledge, skills, and abilities security specialists responsible for protecting Federal facilities in the U.S. should possess and maintain to perform their basic duties and responsibilities. These competencies comprise a range of security disciplines, including physical, personnel, operations, industrial, information, and communications. For security specialists to progress to the full performance level in their specific security disciplines, more in-depth training, experience, and special project assignments must be completed, as appropriate. It is the responsibility of each department and agency to identify and provide any additional site-specific training within the context of its unique mission, policies, operating procedures, and work environment.

4.1 Security and National/Federal Policies and Standards

4.1.1 Interagency Security Committee (ISC)

Security specialists will be knowledgeable in how and why the ISC came into existence, including:

a. State the mission and vision of the ISC;

b. Describe the composition of the ISC; and

c. Be familiar with ISC policies, standards, best practices, and other documents, including, but not limited to:

- Items Prohibited from Federal Facilities: An ISC Standard; and
- Planning and Response to an Active Shooter: An ISC Policy and Best Practices Guide (FOUO).

4.1.2 Facility Security Committees

Security specialists will be knowledgeable in:

a. The ISC standards and policy for convening a facility security committee (FSC); and

b. Roles and responsibilities of the committee members.

4.1.3 ISC Risk Management Process

Security specialists will have a working knowledge of the *Risk Management Process for Federal Facilities: An Interagency Security Committee Standard* as it applies to buildings and facilities in the U.S. occupied by Federal employees for non-military activities, as well as those for which the Secretary of Defense has directed Department of Defense components to adopt ISC standards and guidance documents. This includes the information and requirements set forth by the For Official Use Only (FOUO) Appendices to the *Risk Management Process*: *Design-Basis Threat Report*, *Countermeasures*, and *Child-Care Center Level of Protection Template*.

4.1.4 Crime Prevention through Environmental Design (CPTED)

Security specialists will be able to understand the CPTED principles and how they may be implemented in the design for an effective interior and exterior building environment that reduces fear and deters crime and terrorist activity, to include:

a. Natural surveillance concepts;

b. Territorial reinforcement designs;

c. Natural access control designs; and

d. Facility hardening.

4.1.5 National Infrastructure Protection Plan (NIPP)

Security specialists will be knowledgeable in the concept of critical infrastructure under the NIPP and the need to adequately protect facilities and assets, to include:

a. The vision, mission, and goals for the critical infrastructure community;

b. The partnership structure within which the community undertakes efforts to achieve goals aimed at strengthening security and resilience;

c. The core tenets through description of the principles and assumptions that underpin the NIPP; and

d. The basic framework for risk management activities.

4.1.6 National Fire Protection Association

Security specialists will be knowledgeable of the:

a. National Fire Protection Association (NFPA) 101: Life Safety Code, which addresses construction, protection, and occupancy features necessary to minimize danger to life from the effects of fire (e.g., smoke, heat, and toxic gases);

b. NFPA 70: National Electrical Code (low voltage);

c. NFPA 72: National Fire Alarm and Signaling Code;

d. NFPA 110: Standard for Emergency and Standby Power Systems;

e. NFPA 730: Guide for Premises Security; and

f. NFPA 731: Standard for the Installation of Electronic Premises Security Systems.

4.1.7 All Agency Specific Policies / Standards

Security specialists will be knowledgeable in all applicable agency policies and standards, as well as those issued by the ISC, to include:

a. Operating procedures for physical security;

b. Operating procedures for cyber security, to include industrial systems controls;

c. Operating procedures for personnel security;

d. Operating procedures for information security;

e. Operating procedures for reporting security related violations/suspicious activities;

f. Procedures for occupant emergency plans and all-hazards plans (i.e., active shooter);

g. Procedures for continuity of operations (COOP), to include information systems contingency plans; and

h. Other agency/facility-specific policies, procedures, and standards.

4.2 Facility Security Assessments

4.2.1 Types of Security Assessments

Security specialists will be able to:

a. Conduct recurring security assessments to evaluate threat, vulnerability, and consequence, as well as develop security countermeasures that mitigate risk to an acceptable level;

b. Conduct market survey/pre-lease, new construction, and special assessments; and

c. Demonstrate a general understanding of new site drawings/maps.

4.2.2 Components of a Security Assessment

Security specialists will be able to:

a. Conduct research on and understand content areas and issues such as:

- Law enforcement jurisdiction;
- Crime statistics and trends;
- Natural, design, geographic, and human factors affecting the risk level of the facility;
- ISC FSC policies;
- Funding cycle;
- Historic committee approvals;
- Zoning/Planning committee approvals;
- Internal agency approval process;
- Risk management and mitigation procedures;
- Providing recommendations for defining risk and establishing risk acceptance for the activity/facility, to include those who are involved in the decision process and their respective roles;
- Risk acceptance related to screening and entry control procedures;
- Procedures and rationale for risk acceptance documentation;
- Potential threats using the *ISC Risk Management Process: An ISC Standard, Appendix A: Design-Basis Threat Report* as a guide; and

- Local first responder capabilities (law enforcement, fire, medical) that would service the facility.

b. Conduct analysis such as:
    - Determine the facility security level (FSL) using ISC-approved standards;
    - Complete a physical inspection of grounds and all relevant systems and features;
    - Conduct a lighting survey;
    - Inspect the security officer force (if applicable);
    - Test existing countermeasures;
    - Evaluate pertinent information from tenant interviews;
    - Analyze any additional agency-specific requirements;
    - Evaluate applicable threats and vulnerabilities;
    - Determine impact of loss/consequences;
    - Determine the level of risk to ensure the appropriate corresponding level of protection is provided;
    - Conduct blast analysis; and
    - Interview the following individuals (if applicable):
        - FSC chairperson or security decision maker (for single tenant facilities);
        - A representative of each tenant agency;
        - Building manager;
        - Realty specialist;
        - Facility security personnel;
        - Appropriate law enforcement authorities;
        - Emergency response authorities;
        - Childcare administrators;
        - Housekeeping;
        - Building engineers; and
        - Non-government agencies.

c. Identify and evaluate countermeasures, to include:
    - Evaluate existing countermeasures for their functionality and compliance with ISC standards; and
    - Identify, evaluate, and recommend additional countermeasures, as necessary, to mitigate the risk to an acceptable level.

d. Author a comprehensive, clear, and concise report to document fact-based findings and recommendations determined by the efforts of research and data gathering outlined in this section.

e. Present recommendations outlined in the report generated in this section, including:

   - Explain the security assessment process to FSC or security decision maker (for single tenant facilities) and justify recommended countermeasures; and
   - Demonstrate thorough competency with the use of visual presentation aids.

4.3 Administration (Information) Security

Security specialists will be able to understand:

a. The requirements for classifying, safeguarding, and declassifying national security information, including information relating to defense against transnational terrorism in accordance with E.O. 13526, "Classified National Security Information," and 32 Code of Federal Regulation (CFR) Part 2001-3:

   - Part 1. Original Classification;
   - Part 2. Derivative Classification;
   - Part 3. Declassification and Downgrading;
   - Part 4. Safeguarding;
   - Part 5. Implementation and Review; and
   - Part 6. General Provisions.

b. The requirements for protecting information pursuant to and consistent with applicable law, regulations, and government policies that is not classified, in accordance with existing policies and Federal laws; and

c. The requirements for and ability to conduct compliance inspections and unauthorized disclosure investigations.

4.4 Security of Federal Automated Information Resources

Security specialists will be able to:

a. Identify, review, and assess the physical and environmental protection controls of the National Institute of Standards and Technology (NIST) SP 800-53 & 53A, NIST SP 800-116, and revisions;

b. Understand the Risk Management Framework and the processes used to assess information technology systems and equipment;

c. Demonstrate knowledge and understanding of NIST Security Standards and Guidelines and Federal Information Processing Standard (FIPS) 200; and

d. Demonstrate knowledge and understanding of the Committee on National Security Systems policies and procedures.

4.5 Personnel Security

Security specialists will be able to:

a. Understand the requirements of personnel and national security executive orders and directives, such as:
   - E.O. 10450, *Security Requirements for Government Employment*;
   - E.O. 12968, as amended, *Access to Classified Information*;
   - E.O. 13467, *Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information*;
   - E.O. 13488, *Granting Reciprocity on Excepted Service and Federal Contractor Employees Fitness and Reinvestigating Individuals in High Risk Positions of Public Trust*;
   - Homeland Security Presidential Directive (HSPD) 12;
   - 5 CFR part 731, Suitability Regulations;
   - 5 CFR part 732, Designation of National Security Positions; and
   - Intelligence Community Policy Guidance Number 704.1, 704.2, 704.3, and 704.4 on Investigative Standards, Adjudicative Guidelines, Denials or Revocation of Access to Sensitive Compartmented Information, and Reciprocity.

b. Demonstrate knowledge in the development and execution of the following personnel security policies and/or requirements:
   - Standards for access to classified information and/or assignment to sensitive duties;
   - Criteria for application of suitability and security adjudicative standards;
   - Types and scope of personnel security investigations;
   - Security investigative requirements, special access programs, and reinvestigation;
   - Sensitive and public trust positions;
   - Conducting interviews and due process;
   - Authority to waive investigative requirements;
   - Reciprocity of prior investigations and personnel security determinations; and
   - Procedures for appeals of security clearance denials and revocations.

4.6 Operations Security (OPSEC)

Security specialists will be able to participate in the accomplishment of the following OPSEC objectives:

a. Establish and maintain OPSEC programs to ensure national security-related missions and functions are protected in accordance with National Security Decision Directive 298, *National Operations Security Program*; and

b. Demonstrate a working knowledge of OPSEC programs, to include:

- Assignment of responsibility for OPSEC direction and implementation in an executive department or agency;
- Planning for and implementation of OPSEC in anticipation of and during department or agency activity, when appropriate;
- Use of OPSEC analytical techniques to assist in identifying vulnerabilities and to select appropriate OPSEC measures;
- Enactment of measures to ensure that all personnel, commensurate with their positions and security clearances, are aware of hostile intelligence threats and understand the OPSEC process;
- Perform an annual review and evaluation of OPSEC procedures so as to assist the improvement of OPSEC programs;
- Provision of interagency support and cooperation with respect to OPSEC programs; and
- OPSEC process:
  - Identification of critical information;
  - Analysis of threats;
  - Analysis of vulnerabilities;
  - Assessment of risk; and
  - Application of appropriate OPSEC measure.

4.7 Industrial Security

Security specialists are able to:

a. Understand the requirements of E.O. 12829, as amended by E.O. 12885, that establish a National Industrial Security Program (NISP) to safeguard Federal Government classified information that is released to contractors, licensees, and grantees of the U.S. Government;

b. Demonstrate competence in the execution of the requirements in E.O. 12829 and E.O. 12885 and all the security requirements of the NISP Operating Manual, to include waivers and exceptions to this manual; and

c. Demonstrate knowledge of:

- Industrial, personnel, physical, information technology, and information security policies and procedures;
- Corporate business structures;
- Methods to mitigate foreign ownership, control, and influence;
- Structure of the Committee on Foreign Investments in the U.S.;
- Federal contracting laws and regulations; and
- Facility clearance approval process.

The applicability of the above competencies will be determined by the employee's assignment. These will differ if a security specialist is assigned to one of the NISP Cognizant Security Agencies such as the Defense Security Service, Central Intelligence Agency, Nuclear Regulatory Commission, Department of Energy, or to U.S. Government contracting agencies.

4.8 Personally Identifiable Information (PII)

Security specialists will be able to:

a. Understand the requirements and mandates for identifying, safeguarding, controlling, destroying, and storing of PII, to include:

- The Privacy Act of 1974;
- E.O. 13556, *Controlled Unclassified Information*;
- E-Government Act of 2002 (Title III, the Federal Information Security Management Act);
- Office of Management and Budget (OMB) Circular A-130; and
- Memorandum M-07-16 (Safeguarding Against and Responding to the Breach of PII).

b. Demonstrate reporting procedures for loss or theft of PII.

4.9 Communications Security (COMSEC)

Security specialists will be able to:

a. Understand that U.S. secure communications are controlled and managed under a separate set of security standards and procedures in the National Security Agency Central Security Service Policy Manual No. 3-16;

b. Upon assignment of COMSEC duties, successfully complete the certified COMSEC Custodian course that is recognized by the National Security Agency; and

c. Understand and articulate the following:

- Duties of a COMSEC Custodian;
- Identifying, controlling/storing, and handling of COMSEC material;

- Reporting COMSEC incidents;
- Completing COMSEC forms;
- Ordering COMSEC material/equipment; and
- Destruction procedures of COMSEC.

4.10 Continuity of Operations (COOP)

Security specialists will be able to:

a. Understand the requirements of National Security Presidential Directive-51, HSPD-20, and/or other pertinent policies regarding COOP;

b. Develop a basic COOP plan addressing:
   - Agency essential functions;
   - Alternate facilities and supplies;
   - Delegations of authority and orders of succession;
   - Devolution;
   - Human capital management;
   - Interoperable communications;
   - Reconstitution;
   - Mission critical systems and their contingency plans;
   - Tests, training, and exercises; and
   - Vital records and databases.

c. Understand COOP reporting and national level exercise requirements.

4.11 Facility Security Plans

Security specialists will be able to design a plan that will:

a. Identify security related responsibilities;

b. Identify current and planned security measures;

c. Define building-specific security policies;

d. Contain emergency contacts (such as law enforcement, first responders, security organization, and facility manager);

e. Detail response procedures for emergencies;

f. Outline approved protocols for access by employees, contractors, and visitors;

g. Establish changes in security operations due to temporary upgrades in the National Terrorism Advisory System;

h. Outline the security measure testing schedule performed by the security manager at level IV and V facilities;

i. Identify security support requirements for the Occupant Emergency Plan (OEP);

j. Understand the level of detail to which the plan is written based on the nature of the facility;

k. Protect the plan as FOUO, at a minimum;

l. When applicable, establish protocols with local air traffic control to ensure early notification of threatening flight paths to provide early warning of facility targeting; and

m. Identify response procedures for active shooter/active threat events.

4.12 Occupant Emergency Plan (OEP)

Security specialists will be able to:

a. Understand pertinent Federal Management Regulations (i.e., 102–74.230) and department- or agency-specific policies regarding the OEP;

b. Understand the responsibilities of the security decision maker and Occupant Emergency Organization;

c. Develop an all-hazards OEP, including evacuation plans and shelter-in-place plans; and

d. Test and evaluate an OEP, making appropriate modifications as necessary.

4.13 Incident Management

Security specialists will be knowledgeable of the:

a. Requirements for an Incident Command System (ICS) for managing short-term and long-term field operations for a broad spectrum of emergencies;

b. Organization and operation of unified command in an incident that involves Federal, state, local, and tribal agencies;

c. Key documents that affect planning and operational response in a terrorist attack or weapons of mass destruction incident, including the National Response Plan, National Response Framework, and the National Incident Management System;

d. Reporting requirements and procedures for responding to and managing cybersecurity incidents;

e. Formation and structure of Federal response organizations and how they interface with local emergency response organizations during an emergency incident;

f. ICS operating requirements and components;

g. ICS management concepts/principles;

h. National Terrorism Advisory System; and

i. Minimum ICS Training Level commensurate with the security specialist position and function in normal Emergency Operation Plans.

4.14 Personal Identity Verification (PIV) Card Systems

4.14.1 Personal Identity Verification Card

Security specialists will be able to:

a. Understand PIV credentials defined by the NIST and FIPS 201 or other relevant and recognized standards as an end-point PIV Card;

b. Demonstrate knowledge of identity management; and

c. Work with respective agency's Chief Information Officer to integrate data and databases to common authoritative information technology servers.

4.14.2 Physical Access Control Systems (PACS)

Security specialists will be able to:

a. Understand the requirements of various "off the shelf" physical access control systems that are approved for use under appropriate HSPDs and standards;

b. Understand the architecture of an enterprise system following the recommendations in the NIST SP 800-116 document;

c. Remain current on the General Services Administration (GSA) Schedule 70 where the HSPD-12 products and service providers are centralized and current systems that are used and are compliant with HSPD-12;

d. Write a statement of work to procure and install a system;

e. Commission an installed system; and

f. Use the system as the system administrator.

4.15 Cybersecurity

The security specialist must demonstrate and exercise a functional awareness of the threats, vulnerabilities, and security requirements of information systems towards the enterprise security profile design, to include:

a. Understanding the concept of information systems security and how its infrastructure supports and directly affects the electronic physical access control system (EPACS);

b. Identifying information technology (IT)-based vulnerabilities and inherent threats posed to the enterprise security system (ESS) when connected to a networked IT system;

c. Identifying security countermeasures that reduce Information Security and IT-based threats and vulnerabilities towards the ESS/EPACS;

d. Demonstrate knowledge of IT security architecture and design (e.g., firewalls, intrusion detection systems [IDS], virtual private networking, and virus protection technologies);

e. Apply security risk assessment methodology to building and security systems in accordance with NIST Risk Management Framework, ISC standards, and Department of Homeland Security (DHS) Directives;

f. Demonstrating, during the security design process, the ability to address information systems security requirements and information processing standards for network security, encryption, logical access, and technical capabilities (i.e., FIPS-201, FIPS-140-2, FIPS-197, etc.) in coordination with information technology security specialists;

g. Demonstrate knowledge of Presidential Policy Directive (PPD)-21, to assist in establishing a baseline of our understanding of the volume, timing, and target of cyber operations, including cybercrime, criminal hacker threats, and nation-state espionage, against the networks and systems of the Federal Government facilities' critical infrastructure key resources;

h. Homeland Security Presidential Directives (HSPD);

- HSPD-12 – U.S. policy to eliminate variations in the quality and security of identification used to gain access to secure facilities. A mandate to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees). This directive requires a Federal standard for secure and reliable forms of identification; and
- HSPD-24 – Establishes a framework to ensure that Federal executive departments and agencies use mutually compatible methods and procedures in the collection, storage, use, analysis, and sharing of biometric and associated biographic and contextual information of individuals. Biometrics for identification management and multi-factor unique screening capabilities to enhance our national security.

i. Federal Information Processing Standards (FIPS);

- FIPS-140.2 – This standard specifies the security requirements that will be satisfied by a cryptographic module utilized within a security system protecting sensitive but unclassified information (hereafter referred to as sensitive information);
- FIPS-197 – The Advanced Encryption Standard (AES) specifies a FIPS-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. The AES algorithm is capable of using cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data in blocks of 128 bits; and
- FIPS-201.2 – Designed to satisfy the technical requirements of HSPD-12. NIST-developed standard that specifies PIV requirements for Federal employees and contractors to have access to facilities and information systems. The SmartCard Interagency Advisory Board has indicated that to comply with FIPS 201 PIV II U.S. Government agencies should use Smart Card technology.

j. HSPD-12/FIPS-201 Identity Management; and

k. Federal Information Security Modernization Act (FISMA) of 2014 requires organizations to ensure that all users of information and IT are aware of their cyber security responsibilities. FISMA also requires departments and agencies to identify and train those

with “significant responsibilities for information security.” The Office of Personal Management (OPM) specifies “role-specific training in accordance with NIST standards and guidance.”

4.16 Basic Physical Security Countermeasures

Security specialists will be able to understand the theory and application of physical protection systems to include the six security criteria listed in the ISC’s *Risk Management Process: An ISC Standard, Appendix B: Countermeasures* (site, structure, facility entrance, interior, security systems, and security operations and administration). This includes the primary functions of detection, delay, and response and the secondary function of deterrence, including the following:

a. Understand the concepts and considerations in the integration of physical protection system elements;

b. Demonstrate knowledge of the applicable codes and standards pertaining to physical protection systems;

c. Understand the basic concepts of the procurement process as related to security requirements and enhancements;

d. Read and understand a project schedule, such as a Gantt chart or network diagram;

e. Test countermeasures to assure their functionality;

f. Understand electronic system communication methods, line supervision, cable types, multiplexing, network topologies, and computer peripherals;

g. Read, understand, and evaluate blueprints; and

h. Design a basic statement of work for installation and repair of countermeasures.

4.16.1 Intrusion Detection Systems (IDS)

Security specialists will be able to:

a. Understand the concepts of alarm communication and display and the different technologies available;

b. Understand IDS performance characteristics (i.e., probability of detection, nuisance alarm rate, and vulnerability to defeat);

c. Understand the differences between active and passive sensors, overt and covert sensors, and volumetric and line detection sensors;

d. Identify discrepancies in line supervision by inspecting sensor and control panel terminations;

e. Demonstrate knowledge of the American National Standards Institute and Underwriters Laboratory standards for IDS pertaining to monitoring and hardware; and

f. Understand the requirements and mandates for identifying, safeguarding, controlling, destroying, and storing of PII with IDS, to include: the NIST Special Publication 800-53 rev 4, Security and Privacy Controls for Federal Information Systems and Organizations, and FISMA.

4.16.2 Access Control Systems

Security specialists will be able to:

a. Explain the basic elements of an access control system, how to specify a system, and describe the concept of "defense in depth" or concentric rings;

b. Understand basic objectives of an access control system (i.e., permit only authorized individuals to enter/exit, prevent entry of prohibited items, and facilitate security assessment and response regarding anomalies);

c. Specify appropriate portal types, barriers, or lock hardware for a particular application based on security needs, physical environment, and organizational culture;

d. Understand the basic concepts of and challenges involved in implementing anti-tailgating and anti-pass back policies;

e. Understand the various methods of identity verification and the effectiveness of each type, per HSPD-12;

f. Understand the basic differences between various coded-credential technologies;

g. Understand the different types of biometric technologies available;

h. Demonstrate a basic understanding of the various lock types and lock components; and

i. Understand the factors to be considered in establishing access control needs, requirements, and procedures.

4.16.3 Closed Circuit Television (CCTV)

Security specialists will be able to:

a. Understand the objectives and theory of CCTV systems;

b. Understand the purpose of using video monitoring in security and specify the correct camera type for the appropriate application;

c. Understand the basic components of analog and digital CCTV systems;

d. Understand the different types of cameras and lenses;

e. Understand focal length and field of view;

f. Understand appropriate implementation of pan, tilt, and zoom cameras;

g. Understand analog and digital recording pertaining to resolution, bandwidth, and frame rates;

h. Understand causes of video loss and electromagnetic interference;

i. Demonstrate a basic understanding of fiber-optic video equipment and media converting devices;

j. Understand the direct relationship with protective lighting on camera images. This includes illumination intensity and evenness required for specific cameras as well as color rendition and reflectance of various light types on different surfaces;

k. Demonstrate a basic understanding of the legal considerations associated with video monitoring system applications; and

l. Explain the advantages of CCTV system integration with other physical protection system elements.

4.16.4 Biometrics

Security specialists will be able to understand:

a. Basic biometrics concepts, principles, and applications; and

b. The advantages of using biometric capabilities in security processes.

4.16.5 Protective Lighting

Security specialists will be able to understand:

a. Basic security lighting concepts, principles, and applications;

b. The relationship between video equipment and the various security lighting technologies; and

c. The security standards for exterior security illumination.

4.16.6 Security Barriers

Security specialists will be able to:

a. Understand the different types of security barriers and the security considerations associated with each one; and

b. Determine effective placement of security barriers.

4.16.7 Storage/Safes

Security specialists will be able to:

a. Understand the requirements and specifications for security containers and safes;

b. Demonstrate a basic understanding of the different types of security containers and safes;

c. Understand E.O. 13526, the safeguarding portion of Information Security Oversight Office Implementing Directive, 32 CFR Part 2001-3, pertaining to safeguarding classified information; and

d. Understand Federal specifications for GSA-approved security containers.

4.16.8 Security Locks and Locking Devices

Security specialists will be able to:

a. Understand the basic features of common mechanical and electrical locks;

b. Recognize the differences between regular and high security locks;

c. Understand the lock requirements for restricted areas and locations;

d. Understand the elements of an effective key control system;

e. Demonstrate a basic understanding of fixed and changeable combination locks;

f. Demonstrate a basic understanding of the different types of locks, lock specifications, and hardware requirements; and

g. Understand Federal Specification FF-L-2740B for GSA-approved locks.

4.16.9 Crime Prevention and Security Awareness

Security specialists will be able to:

a. Understand crime prevention as well as security awareness concepts and principles;

b. Demonstrate a basic understanding of CPTED concepts and principles; and

c. Deliver crime prevention and security awareness presentations in oral and written formats.

4.16.10 Security Force Specification and Management

Security specialists will be knowledgeable in:

a. The design of a proper security force per operating requirements;

b. The research required identifying Federal, state, tribal, and local licenses requirements;

c. The legal capabilities and limitations of a security force;

d. The administration or oversight of the security force;

e. Developing standard operating procedures, to include post orders for the security force; and

f. The ISC's *Best Practices for Armed Security Officers in Federal Facilities.*

4.16.11 Inspections

Security specialists will be able to understand the application, limitations, and basic operating principles of:

a. Electronic and trace/vapor detection;

b. Explosive detection devices;

c. Inspection mirrors;

d. Metal detectors;

e. X-ray screening equipment; and

f. Body composition technology.

4.17 Communication Skills

4.17.1 Report Writing

Security specialists will be able to:

a. Write letters, memos, outlines, executive summaries, and local, regional, or department/agency-level policy documents that comply with higher-level guidance, considering the various affecting facets of a particular security issue; and

b. Organize his or her thoughts and write high-impact reports and proposals.

4.17.2 Verbal Communication

Security specialists will be able to:

a. Present technical information in a clear and concise manner;

b. Provide professional responses and feedback; and

c. Effectively network and work with other government agencies and private companies.

4.17.3 Problem Solving/Decision-Making

Security specialists will be able to demonstrate how to resolve complex problems with minimum supervision and:

a. Uncover and define the problem and potential causes;

b. Identify alternatives for approaches to resolve the problem;

c. Select an approach to resolve the problem;

d. Plan the implementation of the best alternative (action plan);

e. Monitor the implementation of the plan;

f. Verify whether the problem has or has not been resolved; and

g. Review reports of investigation to make the adjudicative determination.

4.18 Contracting Administration

4.18.1 Contracting Officer's Representative/Technical Representative (COR/COTR)

Security specialists will be able to:

a. Demonstrate a basic understanding of COR and COTR duties and responsibilities as outlined within the respective agencies requirements;

b. Understand the facility clearance approval process;

c. Understand the requirements for making a Foreign Ownership, Control, or Influence determination for contractors;

d. Work with agency contracting staff to monitor various types of contracts, such as guard service, construction, countermeasure implementation, etc.;

e. Successfully complete training concerning the GSA Supply Schedule;

f. Successfully complete project management training program;

g. Prepare statements of work, limited source justifications, and acquisition plans after completion of formal training and detail assignment in the agency's contracting office;

h. Learn how to commission projects and understand how to closeout a project.

4.19 Administrative Skills

Security specialists possess and maintain a functional working knowledge of systems and applications in the following areas:

a. Architectural drawings;

b. Classified communications technology [i.e., Classified Networks, Homeland Secure Data Network (HSDN), Fax, etc.];

c. Databases;

d. Presentations;

e. Project management;

f. Security assessments;

g. Spreadsheets; and

h. Word processing.

4.20 Health and Safety

Security specialists will be knowledgeable in:

a. Basic First Aid, Cardiopulmonary Resuscitation, Automated External Defibrillator, to include certification;

b. Approved personal protective equipment, especially respiratory protective equipment and the National Institute of Occupational Safety and Health (NIOSH) (www.cdc.gov/niosh) Certification List, particularly of Chemical, Biological, Radiological, and Nuclear equipment;

c. The four levels of emergency responder protection (Levels A, B, C, and D) as found in Occupational Safety and Health Administration (OSHA) Hazardous Waste Operations and Emergency Response, 29 CFR 1910.120 (www.osha.gov), and obtain the required 40 hours of training, if necessary;

d. OSHA Blood-borne Pathogen Standard, 29 CFR 1910.1030 (www.osha.gov), and protective measures when administering first aid;

e. OSHA Hazardous Communication Standard, 29 CFR 1910.1200 (www.osha.gov), and be able to read and understand a Material Safety Data Sheet and other chemical labels;

f. The latest Federal Pandemic Influenza Plan (www.hhs.gov/pandemicflu/plan); and

g. The NIOSH Pocket Guide to Chemical Hazards (current edition) available both in hardcopy and on-line at (www.cdc.gov/niosh).

5.0 List of Abbreviations/Acronyms/Initializations

Abbreviation	Term
ACS	Access Control Systems
AES	Advanced Encryption Standard
CBT	Computer-based Training
CCTV	Closed Circuit Television
CFIUS	Committee on Federal Investments in the United States
CFR	Code of Federal Regulations
COMSEC	Communications Security
COOP	Continuity of Operations
COR	Contracting Officer's Representative
COTR	Contracting Officer's Technical Representative
CPTED	Crime Prevention through Environmental Design
DBT	Design-Basis Threat
DHS	Department of Homeland Security
EO	Executive Order
EPACS	Electronic Physical Access Control System
ESS	Enterprise Security System
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Modernization Act
FOUO	For-Official-Use-Only
FSC	Facility Security Committee
FSL	Facility Security Level
GSA	General Services Administration
HSDN	Homeland Secure Data Network
HSPD	Homeland Security Presidential Directive
ICS	Incident Command System

Abbreviation	Term
IDS	Intrusion Detection System
ISC	Interagency Security Committee
IT	Information Technology
NFPA	National Fire Protection Association
NIMS	National Incident Management System
NIOSH	National Institute of Occupational Safety and Health
NIPP	National Infrastructure Protection Plan
NISP	National Industrial Security Program
NIST	National Institute of Standards and Technology
NRF	National Response Framework
NRP	National Response Plan
NTAS	National Terrorism Advisory System
OEP	Occupant Emergency Plan
OMB	Office of Management and Budget
OPM	Office of Personnel Management
OPSEC	Operations Security
OSHA	Occupational Safety and Health Association
PII	Personally Identifiable Information
PIV	Personal Identification Verification
PPD	Presidential Policy Directive
RCMA	Remote-controlled Model Aircraft
STU	Secure Telephone Units
UAS	Unmanned Aerial System

6.0 Glossary of Terms

Term	Definition
Campus	Two or more Federal facilities located on site and typically sharing some aspects of the environment, such as parking, courtyards, private vehicle access roads, or gates and entrances to connected buildings. A campus also may be referred to as a "Federal center" or "complex."
Classroom Training	Structured learning that takes place in a classroom setting, normally instructor-led, and may vary in format and type of activity depending upon content and time available. Generally, most effective when followed by on-the-job or laboratory experiences that reinforce learning and provide opportunities for practice.
Computer-Based Training	Structured learning that is self-paced and takes place at a personal computer. Computer-based training (CBT) can play a key role in closing skill gaps and improving on-the-job performance. CBT is extremely versatile and more time efficient because employees are not required to spend the full training time in a formal classroom. CBT also includes both CD-ROM and web-based trainings that allow for additional avenues for employees to reach material owned by their organization and available for training or review at any time.
Developmental Activity	Training, education, or other developmental assignments (e.g., reading reference material) that expands upon the knowledge, skills, and abilities to perform current and future duties and accomplish developmental objectives.
Development Needs Assessment	A systematic process by which the supervisor and employee identify the employee's specific developmental activities and priorities based on a review of the position description, job analysis, performance appraisal, organizational goals and objectives, and analysis of the employee's experience, training history, and career development goals.
Development of Job Aids	Formulating a list of procedures, a list of references, or other brief documentation targeted to help the individual more effectively perform a job or task.

Term	Definition
Distance Learning	Any approach to education delivery that replaces the same-time, same-place, face-to-face environment of the traditional classroom.
Facility	Space built or established to serve a particular purpose. The facility is inclusive of a building or suite and associated support infrastructure (e.g., parking or utilities) and land.
Facility Security Plan	A plan that provides direction to key personnel on the security management and policies of a building or facility.
Goal	Something pertinent to an employee's work and career aspirations, such as mastering a skill in their current job or attaining a higher position. The goal should imply some work and challenge, but it should not be so high that it cannot be reasonably obtained. Short range goals are planned to be accomplished within one to two years, and long range goals are planned to be accomplished with three to five years.
Knowledge, Skills, and Abilities	Knowledge is an organized body of information, usually of a factual or procedural nature. Skills are the proficient verbal or mental manipulation of data, people, or things that are observable, quantifiable, and measurable. Ability is the power to perform an activity at the present time. Generally, knowledge pertains to the mastery of a subject matter area, skill pertains to physical or mental competence, and ability pertains to the potential for using knowledge or skill when needed.
Learning Objective	A brief description of the knowledge, skills, and abilities, expressed in behavioral terms, the employee will be expected to achieve on completion of the training.
Objective	Something worthwhile to obtain that is pertinent to the employee's work and career. Developmental objectives should be as specific as possible (e.g., to demonstrate how to evaluate computer systems with multilevel security features).
On-the-Job-Training	Training that is conducted and evaluated in the work environment.

Term	Definition
Reading or Research Project	Review of the specified set of readings on a topic or the completion of a research project and resulting report.
Rotational Assignment/Detail	Temporarily placing an individual in a different job and/or work environment where he or she has the opportunity to learn and develop specific skills that may complement or be needed for his or her regular job.
Security Specialist	Includes positions where the primary duties of which are analytical, planning, advisory, operational, or evaluative work that has as its principal purpose the development and implementation of policies, procedures, standards, training, and methods for identifying and protecting information, personnel, property, facilities, operations, or material from unauthorized disclosure, misuse, theft, assault, vandalism, espionage, sabotage, or loss. Duties involve the management, supervision, or performance of work in: (1) developing, evaluating, maintaining, and/or operating systems, policies, devices, procedures, and methods used for safeguarding information, property, personnel, operations, and materials; and/or (2) developing and implementing policies and procedures for analyzing and evaluating the character, background, and history of employees, candidates for employment, and other persons having or proposed to be granted access to classified or other sensitive information, materials, or work sites.
Self-Study Program	Learner-controlled experience generally involving the use of prepared materials and a self-paced structure with options for sequencing and level of detail required. This type of activity is appropriate when self-study materials are available; the number of people needing the training is small; individual backgrounds and needs vary; and an individual will benefit from a customized schedule of instruction. Also, appropriate when large numbers of individuals need training but cannot be easily assembled in the same place at the same time. Subject matter that is enhanced through the synergism of trainer-participant interaction is not recommended as part of a self-study program.

Term	Definition
Shadowing	Learning through first observing the work of a qualified individual and then practicing the application of the same skill or set of skills, followed by feedback and evaluation.
Simulation Training	The application of classroom or other learning in a realistic but not actual situation in which the participant can practice skills. Simulation training may involve the use of specialized equipment or, in some cases, scenarios and role playing.
Structured Discussion	Working with a mentor or other individual to learn a specified topic through discussion. The structure might include preparation of questions for discussion, prerequisite reading, or other research.
Symposium/Conference/Workshop /Seminar	Any of a variety of informational, instructional, and/or interactive events focusing on a specific topic or area of concern.

7.0 References

- Executive Order 12977, as amended by Executive Order 13286
- Items Prohibited from Federal Facilities: An ISC Standard
- Planning and Response to an Active Shooter: An ISC Policy and Best Practices Guide (FOUO)
- Risk Management Process for Federal Facilities: An ISC Standard
- Risk Management Process: the Design-Basis Threat Report (FOUO)
- Risk Management Process: Countermeasures (FOUO)
- Risk Management Process: Child-Care Center Level of Protection Template (FOUO)
- National Fire Protection Association 101: Life Safety Code
- National Fire Protection Association 70: National Electrical Code
- National Fire Protection Association 72: National Fire Alarm and Signaling Code
- National Fire Protection Association 110: Standard for Emergency and Standby Power Systems
- National Fire Protection Association 730: Guide for Premises Security
- National Fire Protection Association 731: Standard for the Installation of Electronic Premises Security Systems
- Executive Order 13526, "Classified National Security Information"
- 32 CFR Part 2001-3
- National Institute of Standards and Technology, SP 800-53 & 53A
- National Institute of Standards and Technology, SP 800-116
- National Institute of Standards and Technology, Security Standards and Guidelines
- Federal Information Processing Standard 200
- Executive Order 10450, *Security Requirements for Government Employment*
- Executive Order 12968, as amended, *Access to Classified Information*
- Executive Order 13467, *Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information*
- Executive Order 13488, *Granting Reciprocity on Excepted Service and Federal Contractor Employees Fitness and Reinvestigating Individuals in High Risk Positions of Public Trust*
- Homeland Security Presidential Directive-12
- 5 CFR part 731, *Suitability Regulations*

- 5 CFR part 732, *Designation of National Security Positions*
- Intelligence Community Policy Guidance Number 704.1, 704.2, 704.3, and 704.4 on Investigative Standards, Adjudicative Guidelines, Denials or Revocation of Access to Sensitive Compartmented Information, and Reciprocity
- National Security Decision Directive 298, *National Operations Security Program*
- The Privacy Act of 1974
- E.O. 13556, *Controlled Unclassified Information*
- E-Government Act of 2002 (Title III, the Federal Information Security Management Act)
- OMB Circular A-130
- Memorandum M-07-16 (Safeguarding Against and Responding to the Breach of PII)
- National Security Presidential Directive-51
- Homeland Security Presidential Directive-20
- Federal Management Regulations (i.e., 102–74.230)
- National Response Plan
- National Response Framework
- National Incident Management System
- National Terrorism Advisory System
- Federal Information Processing Standard 140.2
- Federal Information Processing Standard 197
- Federal Information Processing Standard IPS-201.2
- Federal Information Security Modernization Act of 2014
- Federal Specification FF-L-2740B
- Best Practices for Armed Security Officers in Federal Facilities
- National Institute of Occupational Safety and Health Certification List
- 29 CFR 1910.120, *OSHA Hazardous Waste Operations and Emergency Response*
- 29 CFR 1910.1030, *OSHA Blood-borne Pathogen Standard*
- 29 CFR 1910.1200, *OSHA Hazardous Communication Standard*
- Federal Pandemic Influenza Plan
- National Institute of Occupational Safety and Health Pocket Guide to Chemical Hazards

Interagency Security Committee Participants

ISC Chair
Robert Kolasky
Acting Assistant Secretary for Infrastructure Protection
U.S. Department of Homeland Security

ISC Program Director
Daryle Hernandez
Interagency Security Committee

ISC Operations Director
Bernard Holt
Interagency Security Committee

2016-2017 Training Subcommittee Chair and Members	
Chair Richard Swengros Federal Protective Service	
Richard Cestero Bureau of Engraving and Printing	Jose Delgado Federal Law Enforcement Training Center
Megan Drohan Interagency Security Committee	Anthony Evernham Interagency Security Committee
Mike Griffin General Services Administration	Reid Hilliard Department of Justice
Bernard Holt Interagency Security Committee	Walter Jones Pentagon Force Protection Agency
Kyle Macken Interagency Security Committee	Rob Marohn Federal Protective Service
Tracy Miller Federal Protective Service	Matthew O'Saben Central Intelligence Agency
Jerry Stanphill Federal Aviation Administration	Mark Strickland General Services Administration
Sandra Wilson Pentagon Force Protection Agency	

ISC Executive Director
Austin Smith
Interagency Security Committee

2011-2012 Working Group Chair and Members	
Chair Dean Hunter Office of Personnel Management	
John J. Cunninghan Office of Personnel Management	Mike DeFrancisco Department of Agriculture
Richard S. Eligan Office of Personnel Management	Ashley Gottlinger Interagency Security Committee
Bernard Holt Interagency Security Committee	Valeria Lee-Lloyd Department of Homeland Security
Jason I. Rosen Office of Personnel Management	Doug Vorwerk Department of Homeland Security