Security Specialist Competencies

An Interagency Security Committee Guideline

1st Edition - January 2012

Homeland Security

ONE SOURCE • ONE AUTHORITY
INTERAGENCY SECURITY COMMITTEE
1995

This page intentionally left blank.

Preface

As Chair of the Interagency Security Committee (ISC), I am pleased to introduce the *Security Specialist Competencies: An Interagency Security Committee Guideline (the Guideline)*. The Guideline provides the range of core competencies Federal security specialists can possess to perform their basic duties and responsibilities.

One of our top national priorities is the protection of all Federal employees and private citizens who work within and visit U.S. Government-owned or leased facilities. Composed of 50 Federal departments and agencies, the ISC's primary mission is to craft security standards and best practices for nonmilitary Federal facilities in the United States.

The ISC's objective was to develop recommendations all Federal agencies could utilize 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 guideline is a significant milestone and represents exemplary collaboration within the ISC working group and across the entire ISC. The ISC will review and update this guideline as needed.

Todd M. Keil
Assistant Secretary for Infrastructure Protection

Table of Contents

1.0 Background 1

2.0 Applicability and Scope 1

3.0 Methodology 1

4.0 Security Specialist Competencies 2

4.1 Security and National/Federal Policies and Standards 2

4.1.1 Interagency Security Committee 2

4.1.2 Facility Security Committees 2

4.1.3 ISC Facility Security Level Determination Standard 2

4.1.4 ISC Risk Management Process 3

4.1.5 ISC's Physical Security Criteria for Federal Facilities Standard and Design-Basis Threat Report 3

4.1.6 Crime Prevention Through Environmental Design (CPTED) 3

4.1.7 National Infrastructure Protection Plan (NIPP) 3

4.1.8 National Fire Protection Association 3

4.1.9 All Agency Specific Policies/Standards 3

4.2 Facility Security Assessments 4

4.2.1 Types of Security Assessments 4

4.2.2 Components of a Security Assessment 4

4.3 Information Security 5

4.4 Security of Federal Automated Information Resources 6

4.5 Personnel Security 6

4.6 Operations Security 7

4.7 Industrial Security 7

4.8 Personal Identifiable Information 8

4.9 Communications Security 8

4.10 Continuity of Operations 9

4.11 Occupant Emergency Plan 9

4.12 Incident Management 9

4.13 Personal Identity Verification (PIV) Card Systems 10

4.13.1 Personal Identity Verification Card 10
4.13.2 Physical Access Control Systems 10
4.14 Basic Physical Security Countermeasures 10
4.14.1 Intrusion Detection Systems 11
4.14.2 Access Control Systems 11
4.14.3 Video Monitoring Systems 12
4.14.4 Biometrics 12
4.14.5 Protective Lighting 12
4.14.6 Security Barriers 13
4.14.7 Storage/Safes 13
4.14.8 Security Locks and Locking Devices 13
4.14.9 Crime Prevention and Security Awareness 13
4.14.10 Security Force Specification and Management 14
4.14.11 Inspections 14
4.15 Communication Skills 14
4.15.1 Report Writing 14
4.15.2 Verbal/Speech 14
4.15.3 Problem Solving/Decision-making 15
4.16 Contracting Administration 15
4.16.1 Contracting Officer's Technical Representative (COTR) 15
4.17 Administrative Skills 15
4.18 Health and Safety 16
4.19 Definitions 17
Interagency Security Committee Participants 19

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 a clear need for consistency in security personnel qualifications and training in today's threat environment. Therefore, based on the Government Accountability Office's request 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 security specialists throughout the Federal government should possess.

The working group's objective was to develop recommendations all agencies could utilize 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 become proficient to a unified, minimum capability. This guidance document reflects the efforts of the working group in working toward that end.

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 the Federal security specialist workforce.

This document provides the range of core competencies that Federal security specialists can 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 document does not cover unique requirements of individual Federal departments and agencies or additional training and certifications for specialized positions such as: a communication security (COMSEC) officer, information security officer, executive protection specialist, or others. The ISC recognizes Federal departments and agencies will implement this guidance in a manner that reflects the unique, varied mission requirements and funding capabilities of their respective components.

3.0 Methodology

This document presents a series of subject areas and the corresponding competencies for each of the subject areas. It is intended that these competencies represent a baseline for all Federal security specialists as they progress toward reaching the full performance level in one or more of the individual security disciplines. Further, it must be noted that the competencies outlined in this document are performance based, specifying the knowledge, skills, and abilities that a

specialist should possess and that would require validation by an individual's manager, rather than a mandate for a specified number of course hours or a particular vendor. A variety of activities can 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 training
- Web-based instruction

4.0 Security Specialist Competencies

The subject areas and competencies identified in this section outline the general knowledge and skills Federal security specialists should possess and maintain to perform their basic duties and responsibilities. For incumbent Federal 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 required. It is the responsibility of each department and agency to require and provide this additional, site-specific training within the context of their unique mission, policies, operating procedures, and work environment.

4.1 Security and National/Federal Policies and Standards

4.1.1 Interagency Security Committee

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

a. State the mission and vision of the ISC; and

b. Describe the composition of the ISC.

4.1.2 Facility Security Committees

Incumbents will be:

a. Knowledgeable in the policy and procedures a Facility Security Committee (FSC) uses when presented with security issues; and

b. Knowledgeable in the roles and responsibilities of the committee members.

4.1.3 ISC Facility Security Level Determination Standard

Incumbents will be able to define the criteria and successfully utilize the process for determining a facility security level (FSL).

4.1.4 ISC Risk Management Process

Incumbents will have a working knowledge of the "ISC Risk Management Process" for Federal buildings and facilities in the United States occupied by Federal employees for nonmilitary activities.

4.1.5 ISC's Physical Security Criteria for Federal Facilities Standard and Design-Basis Threat Report

Incumbents will be able to define and successfully utilize the process for determining the customized security measures required at a specific Federal facility.

4.1.6 Crime Prevention Through Environmental Design (CPTED)

Incumbents will be able to understand the CPTED principles and how they may be implemented in the design of an effective interior and exterior building environment in order to both reduce the fear of potential crime and terrorist activity and encourage desirable behavior to include:

a. Natural surveillance concepts;

b. Territorial reinforcement designs;

c. Natural access control designs; and

d. Facility hardening.

4.1.7 National Infrastructure Protection Plan (NIPP)

Incumbents will be knowledgeable in the concept of critical infrastructure under the NIPP and the need to adequately protect such facilities and assets.

4.1.8 National Fire Protection Association

Incumbents will be knowledgeable of the:

a. National Fire Protection Association (NFPA) 101: Life Safety Code; that addresses those 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 72: National Fire Alarm and Signaling Code;

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

d. NFPA 730: Guide for Premises Security; and

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

4.1.9 All Agency Specific Policies / Standards

Incumbents will be knowledgeable in all their respective agency policies and standards, as well as those issued by the ISC.

4.2 Facility Security Assessments

4.2.1 Types of Security Assessments

Incumbents will be able to:

a. Conduct recurring security assessments:
   - Assessments will evaluate threats, vulnerabilities, and impact of loss/consequences 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

Incumbents will be able to:

a. Conduct Research:

   Research on the facility should be conducted at a minimum on:
   - Law enforcement jurisdiction;
   - Crime statistics and trends;
   - Natural, design, geographic, and human factors affecting the risk level of the facility;
   - Potential threats to include use of the ISC *Design-Basis Threat Report*;
   - Research of emergency services from local fire medical services, and hospital capabilities that would service the facility;

b. Inspect and Analyze:
   - Determine the 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;
   - Interview the following individuals at a minimum:
     - FSC Chairperson or Designated Official;
     - A representative of each tenant agency, if possible;
     - Building Manager;
     - Realty Specialist;
     - Facility security personnel;
     - Appropriate law enforcement authorities;
     - Emergency response authorities;

c. Perform a Threat Assessment:
   - 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;

d. Identify and Evaluate Countermeasures:
   - Existing Countermeasures – Evaluate for their functionality and compliance with ISC Standards;
   - Additional Countermeasures – Identify, evaluate, and recommend, as necessary, to mitigate the risk to an acceptable level;

e. Understand the Countermeasure Approval and Process:
   - ISC Facility Security Committee policies;
   - Funding cycle;
   - Historic Committee approvals;
   - Zoning/Planning Committee approvals;
   - Internal agency approval process;

f. 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 4.2.2;

g. Present recommendations outlined in the report generated in 4.2.2:
   - Explain the security assessment process to FSC or designated authority and justify recommended countermeasures; and
   - Demonstrate thorough competency with the use of visual presentation aids.

4.3 Information Security

Incumbents will be able to understand:

a. The following 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”:
   - Part 1. Original Classification;
   - Part 2. Derivative Classification;
   - Part 3. Declassification and Downgrading;
   - Part 4. Safeguarding;
   - Part 5. Implementation and Review;
   - 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 E.O. 13556, “Controlled Unclassified Information”; and

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

4.4 Security of Federal Automated Information Resources

Incumbents 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

Incumbents 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";
- 5 Code of Federal Regulation (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;

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

Incumbents will be able to participate in the accomplishment of the following Operations Security (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";

b. Demonstrate a working knowledge of an OPSEC program 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, where appropriate, during department or agency activity;
   - 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;
   - Performing 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;
   - Operations Security Process:
     - Identification of critical information;
     - Analysis of threats;
     - Analysis of vulnerabilities;
     - Assessment of risk; and
     - Application of appropriate OPSEC measure.

4.7 Industrial Security

Incumbents will be 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 the above E.O. and all the security requirements of the NISP Operating Manual to include waivers and exceptions to this manual;

c. Examples of competencies required:
   - Apply knowledge of industrial, personnel, physical, IT, and information security policies and procedures;

- Apply knowledge of corporate business structures;
- Apply or understand methods to mitigate foreign ownership, control, and influence;
- Understand the structure of the Committee on Foreign Investments in the U.S.;
- Apply knowledge of Federal contracting laws and regulations; and
- Apply knowledge of the 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 Personal Identifiable Information

Incumbents will be able to:

a. Understand the requirements and mandates for indentifying, safeguarding, controlling, destroying, and storing of Personally Identifiable Information (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;
   - Memorandum M-07-16 (Safeguarding Against and Responding to the Breach of PII); and

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

4.9 Communications Security

Incumbents will be able to:

a. Understand that the United States' 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;

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

Incumbents will be able to:

a. Understand the requirements of National Security Presidential Directive-51, Homeland Security Presidential Directive (HSPD) -20, and/or other pertinent policies regarding Continuity of Operations (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;
   - Tests, training, and exercises;
   - Vital records and databases; and

c. Understand COOP reporting and national level exercise requirements.

4.11 Occupant Emergency Plan

Incumbents will be able to:

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

b. Understand the responsibilities of the Designated Official and Occupant Emergency Organization;

c. Develop an All-Hazards Occupant Emergency Plan (OEP) including evacuation plans and shelter-in-place plans; and

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

4.12 Incident Management

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

e. ICS operating requirements and components;

f. ICS management concepts/principles;

g. National Terrorism Advisory System; and

h. Minimum ICS Training Level commensurate with the Security Specialist position and function in normal Emergency Operation Plans.

4.13 Personal Identity Verification (PIV) Card Systems

4.13.1 Personal Identity Verification Card

Incumbents will be able to:

a. Understand PIV credentials defined by the NIST and FIPS 201 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.

4.13.2 Physical Access Control Systems

Incumbents will be able to:

a. Understand the requirements of various physical access control systems ("off the shelf") that are approved for use under HSPD-12, FIPS 201;

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;

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.

4.14 Basic Physical Security Countermeasures

Incumbents will be able to understand the theory and application of physical protection systems. 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; and

g. Read, understand and evaluate blueprints.

4.14.1 Intrusion Detection Systems

Incumbents will be able to:

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

b. Understand intrusion detection system 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; and

e. Demonstrate knowledge of the American National Standards Institute and Underwriters Laboratory standards for Intrusion Detection Systems pertaining to monitoring and hardware.

4.14.2 Access Control Systems

Incumbents will be able to:

a. 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);

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

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

d. Understand the various methods of identity verification and the effectiveness of each type;

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

f. Understand the different types of biometric technologies available;

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

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

4.14.3 Video Monitoring Systems

Incumbents will be able to:

a. Understand the objectives and theory of video monitoring 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 video monitoring 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 recording requirements 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 video monitoring system integration with other physical protection system elements.

4.14.4 Biometrics

Incumbents will be able to understand basic biometrics concepts, principles, and applications.

4.14.5 Protective Lighting

Incumbents will be able to understand:

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

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

c. The security standards for exterior security illumination.

4.14.6 Security Barriers

Incumbents 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.

4.14.7 Storage/Safes

Incumbents 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, pertaining to safeguarding classified information; and

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

4.14.8 Security Locks and Locking Devices

Incumbents 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 specialized rooms 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-2740 for GSA-approved locks.

4.14.9 Crime Prevention and Security Awareness

Incumbents 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.

4.14.10 Security Force Specification and Management

Incumbents 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; and

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

4.14.11 Inspections

Incumbents will be able to understand the use, limitations, and basic operating principles of:

- Electronic and trace/vapor detection;
- Explosive detection devices;
- Inspection mirrors;
- Magnetometers;
- Metal detectors; and
- X-ray screening equipment.

4.15 Communication Skills

4.15.1 Report Writing

Incumbents 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.

4.15.2 Verbal/Speech

Incumbents will be able to:

a. Present 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.

4.15.3 Problem Solving/Decision-making

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

- Uncover and define the problem and potential causes;
- Identify alternatives for approaches to resolve the problem;
- Select an approach to resolve the problem;
- Plan the implementation of the best alternative (action plan);
- Monitor the implementation of the plan;
- Verify whether the problem has or has not been resolved; and
- Review reports of investigation to make the adjudicative determination.

4.16 Contracting Administration

4.16.1 Contracting Officer's Technical Representative (COTR)

Incumbents will be able to:

a. Demonstrate a basic understanding of the COTR's 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 on monitoring 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 following the *Project Manager's Body of Knowledge* curriculum;

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

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

4.17 Administrative Skills

Incumbents will be able to possess and maintain a functional working knowledge of information technology applications in the following areas:

- Architectural drawings;
- Classified communications technology [Secure Telephone Units (STUs), Homeland Secure Data Network (HSDN), Fax, etc.];
- Databases;
- Presentations;

- Project management;
- Security assessments;
- Spreadsheets; and
- Word processing.

4.18 Health and Safety

Incumbents will be knowledgeable in:

a. 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;

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

c. OSHA Bloodborne Pathogen Standard, 29 CFR 1910.1030 (www.osha.gov), and protective measures when administering first aid;

d. 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;

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

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

This space intentionally left blank.

4.19 Definitions

Classroom Training: Structured learning that takes place in a classroom setting that varies 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 as 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.

Distance Learning: Any approach to education delivery that replaces the same-time, same-place, face-to-face environment of the traditional classroom.

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 summary of knowledge, skills, and abilities the employee will be expected to achieve.

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 learn to evaluate computer systems with multilevel security features).

On-the-Job-Training: Training that is conducted and evaluated in the work environment.

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.

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.

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.

Interagency Security Committee Participants

ISC Chair

Todd M. Keil

Assistant Secretary for Infrastructure Protection

U.S. Department of Homeland Security

ISC Executive Director

Austin Smith

Interagency Security Committee

Office of Infrastructure Protection

U.S. Department of Homeland Security

Working Group Chair and Members	
Chair Dean Hunter – OPM	
Richard S. Eligan – OPM	Jason I. Rosen – OPM
John J. Cunninghan – OPM	Valeria Lee-Lloyd – DHS
Mike DeFrancisco – USDA	Doug Vorwerk – DHS
Bernard Holt – ISC	Ashley Gotlinger – ISC