INTERAGENCY SECURITY COMMITTEE

SECURITY SPECIALIST CAREER PROGRESSION LADDER

An Interagency Security Committee Guide

2022 Edition

U.S. Department of Homeland Security
Cybersecurity and Infrastructure Security Agency
Interagency Security Committee

Message from the Chief

The Interagency Security Committee (ISC) vision statement is: "*Federal facilities, the people who work at them, and those who visit them are safe and secure throughout the country*." The ISC achieves its vision by establishing security policies, ensuring compliance, and enhancing the quality and effectiveness of the security and protection of federal facilities. The ISC is chaired by the Cybersecurity and Infrastructure Security Agency (CISA), Executive Assistant Director for Infrastructure Security, and consists of 66 departments and agencies working collaboratively.

As Chief of the ISC, I am pleased to introduce *Security Specialist Career Progression Ladder: An Interagency Security Committee Guide*. This document is intended to be a companion document to the *Security Specialist Competencies: An Interagency Security Committee Guide, 2017 edition,* which provides the range of core competencies federal security specialists should possess to perform their basic duties and responsibilities. An exemplary collaboration within the ISC Training Subcommittee and across the entire ISC, this guide lays out a road map for federal security specialists to develop their individual career paths and supports supervisors in their own career enhancement and career-counseling efforts.

Daryle J. Hernandez
Chief, Interagency Security Committee
Cybersecurity and Infrastructure Security Agency

Table of Contents

1.0 Introduction

Security specialists work in a variety of functional areas such as personnel security, physical security, information security, operations security, cybersecurity, and industrial security. The federal security specialist is concerned primarily with the protection of sensitive or classified information, personnel, facilities, resources, or processes against criminal, terrorist, or hostile intelligence activities. Duties may also include the management, supervision, or performance of security-related work.

As with any career, security specialists can enhance their job satisfaction, and organizational commitment through strategic planning and professional development. However, they are often unaware of available options and resources to help them reach their career goals, which may include:

- **Advancement:** Moving to a higher position
- **Lateral move:** Moving across functions to develop skills
- **Changing to a lower grade:** Changing to a lower grade for developmental purposes [Note: Employees are entitled to pay retention only if the training program is a formal government-wide training program, such as upward mobility, apprenticeship, or career internship.]
- **Mobility:** A geographical move to obtain developmental experiences to advance to desired grades
- **Job enrichment**: Working towards greater responsibility and variety in the present position
- **Exploratory research:** Actively investigating other options or taking temporary special projects or assignments to explore a new area
- **Projected outcome:** Calculating the risks attached to various actions in the career plan [Note: Risk includes the possibility of failure, as well as the potential loss of something that individuals value, such as comfortable habits or a high confidence level.]
- **Cross-training:** Opportunities to ensure staff can perform multiple jobs across the organization

The Security Specialist Career Progression Ladder: An Interagency Security Committee Guide is intended to serve as a roadmap for the professional development of federal security specialists as they seek to:

- Identify goals, pinpoint areas for growth, and create a plan for success.
- Understand core and technical competencies.
- Discover training and professional development opportunities to build skills and maximize potential.

2.0 Background

In October 1995, presidential Executive Order (EO) 12977[1] established the ISC, which has developed and published over 20 policies, standards, and recommendations to identify, assess, and prioritize risks at federal facilities. In May 2007, EO 13434 *National Security Professional Development* requires "The head of each agency with national security functions shall (a) identify and enhance existing national security professional development programs and infrastructure, and establish new programs as necessary, in order to fulfill their respective missions to educate, train, and employ security professionals consistent with the National Strategy."

To assist with compliance of EO 12977[2] and EO 13434, in 2017, the ISC published the *Security Specialists Competencies: An ISC Guide, 2nd Edition* to provide a range of core competencies federal security specialists should possess to perform their basic duties and responsibilities. Since its publication, the ISC identified the need to further develop a common baseline of knowledge and abilities specific to security specialists and reengaged the Training Subcommittee to develop the *Security Specialist Career Progression Ladder: An Interagency Security Committee Guide*.

3.0 Applicability

Pursuant to the authority provided to the ISC in Section 5 of EO 12977[3], as amended by EO 13286, this ISC document provides guidance on developing educational and training initiatives to improve the competencies and career progression of security specialists and their supervisors within federal departments and agencies.

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.

4.0 Security Specialist Career Development

Career development helps both the individual and the organization. Organizations that offer clearly defined roles and required competencies for every position and that aid in proper planning, may then develop employees that feel valued and supported. Encouraged by this demonstration, employees may develop buy-in and a sense of belonging as they align their knowledge, skills, and interests with current and future possibilities, which can lead to increased commitment to the organization.

Aimed at sustaining or improving confidence and productivity through increased motivation, responsibilities, and job satisfaction, career development programs should meet three objectives:

---

[1] On Nov 27, 2023, the President signed EO 14111, *Interagency Security Committee* superseding EO 12977. EO 14111 reinforces the importance of the security of federal facilities in the face of persistent and emerging threats.
[2] Ibid.
[3] Ibid.

- Provide employees a chance to evaluate their needs, interests, and skills in relation to career opportunities inside and possibly outside of their career field
- Assist employees in developing short and long-range goals
- Explore ways and resources to meet those goals

Each security specialist is responsible for their own career planning and professional development, whether its advancement to higher positions, enrichment of their current position, or enhancement of their skills to keep up with evolving technologies. However, they are not alone in the process as a supervisor can offer valuable perspectives on employees' abilities and job performance, identify when employees are underutilized, and provide ways to expand their responsibilities, creating a better fit between the employee and the organization.

A supervisor's function is also to support, guide, and encourage the development and growth of employees' knowledge and skills and bring individual and organizational goals into alignment. By sharing their own experience and organizational knowledge, supervisors can provide resources and access to job and career development information. However, supervisors must avoid promising specific job opportunities, raising employees' hopes, or projecting their own expectations on employees' career objectives.

The career development process involves self-reflection and supervisory observation, both of which can help employees identify gaps in experience, knowledge, or abilities that limit effective performance. Figure 1 lists some areas for consideration when reflecting on and determining employee preferences while Figure 2 offers pertinent training and education questions an employee may ask to identify any gaps and to assist in reaching their full potential.

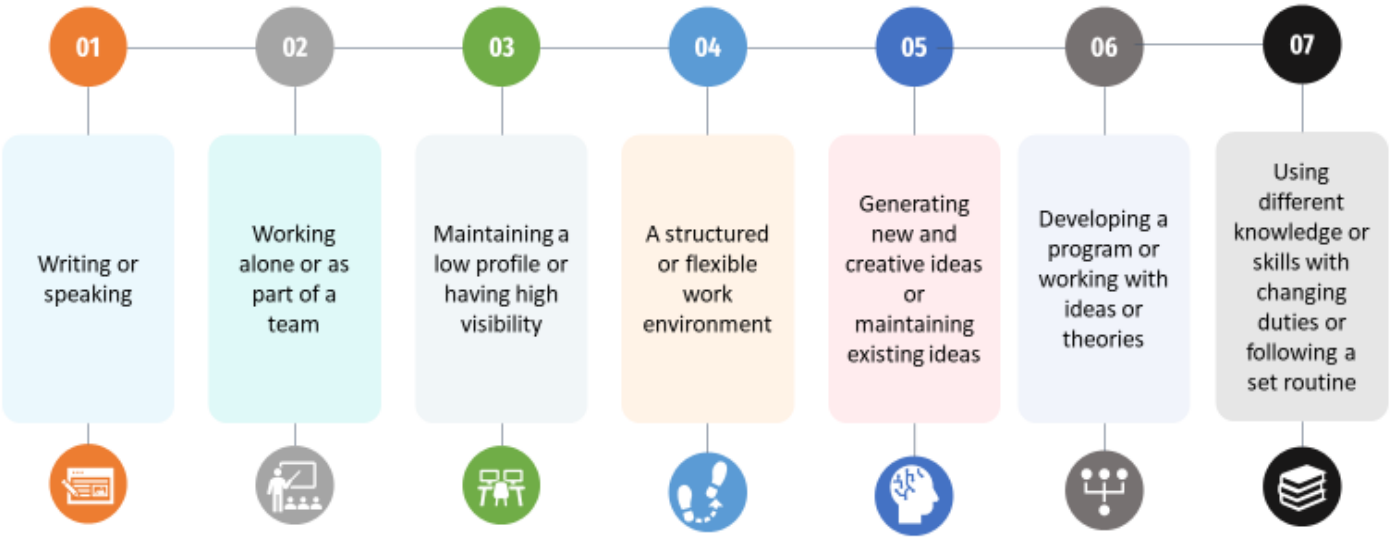

Figure 1: Employee Areas for Consideration

Figure 2: Training and Education Considerations

Employees often see promotion as the primary goal of career development programs. However, they may be disappointed and frustrated when that is not the case, so providing employees with information on realistic opportunities during the information gathering process is helpful. Questions that supervisors should be prepared to address include:

- What are the prospects for promotion or transfer from the present job?
- What percentages of employees reach a certain target level in the organization?
- Where is the fastest growth and, therefore, best promotion opportunity?
- If an employee reaches a promotion ceiling, what career paths or opportunities exist for the employee to continue career advancement (such as lateral moves to broaden experience)?

5.0 Career Progression Planning Process

To achieve career goals, its crucial to chart a road map (see Figure 3) for success by documenting competencies, assessing proficiency levels, prioritizing competencies, identifying training opportunities, and building an Individual Development Plan (IDP).

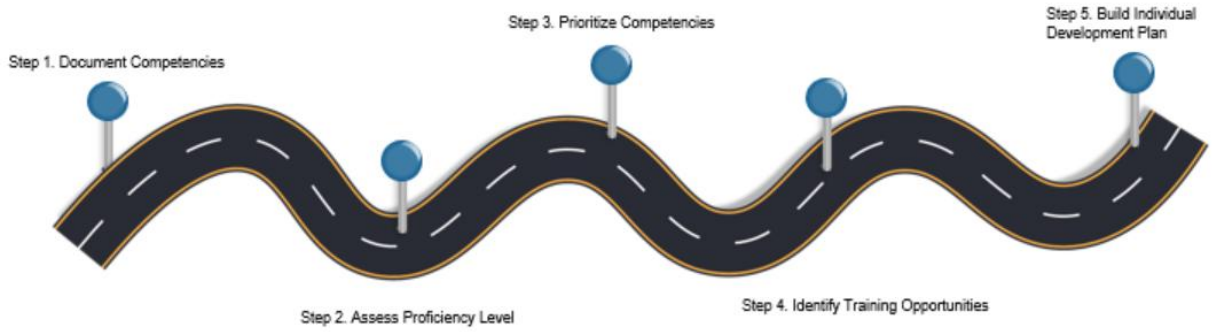

Figure 3: Career Progression Planning Path

Step 1: Document applicable core and technical competencies

Competencies are a combination of the knowledge, skills, abilities, and behaviors that are needed to be successful in a job. They do not define specific tasks or performance standards, but rather expectations about what a security specialist needs to know and do well to perform at a high level. Competencies generally include the following three components:

1. Core competencies, which apply to all security specialists and include areas such as communications and customer service.

2. Technical competencies, which apply to specific jobs and associated tasks such as risk assessments or project planning.

3. Supervisory competencies, such as assigning, monitoring, and evaluating work which enable supervisors to become better leaders and managers.

To identify the relevant competencies for your position and office, review the competencies found in *Appendix A: Recommended Core Competencies* and *Appendix B: Recommended Technical Competencies*. A sample matrix for recording necessary or applicable competencies can be found in *Appendix C: Competency Matrix for Security Specialists*.

After adequately developing and demonstrating primary competencies, security specialists and their supervisors should explore other competencies that will increase employee proficiency and upward mobility. This is an important component of the process since it may be necessary as an employee progresses in their security career.

Step 2: Assess your proficiency level for each competency

As security specialists gain more experience, participate in training, and take on new responsibilities, their knowledge, skills, and abilities will naturally increase leading to greater proficiency. Determining the level of proficiency helps identify where an individual is at and where to focus development efforts without being tied to a specific grade level or years of experience. Table 1 provides a rubric for determining proficiency at the entry, intermediate, or advanced levels.

Table 1: Proficiency Levels

Proficiency Level		
Entry	**Intermediate**	**Advanced**
Able to apply the competency in simple situations. Able to complete tasks on your own after being told or shown how with close or frequent guidance. Able to understand the general principles and concepts related to the competency.	Able to apply the competency in moderately difficult situations with little or no guidance. Able to generally perform tasks independently, with help from time to time. Able to draw conclusions and make recommendations.	Able to apply the competency in difficult situations with no guidance. Able to be recognized as an expert and considered a "go to" person. Able to advise and coach others. You participate in and lead complex discussions on key principles and concepts.

Because the proficiency level required for each competency varies by position, career level, and organizational needs, it's likely security specialists may be at different proficiency levels for different competencies. In these instances, when an employee falls between two levels, use judgment in making the determination. Table 2 provides a simple guide for identifying proficiency levels; however, exercise flexibility in the aforementioned situations.

Table 2: How to Determine Proficiency Level

Proficiency Level	Questions to Ask
Entry	▪ Is the employee able to understand only the basic terminology, concepts, and principles related to this competency? ▪ Are they able to apply them only in simple situations, but struggle in more complicated ones? ▪ Do they often have to seek guidance and support from someone more senior than me?
Intermediate	▪ Do they possess a solid understanding of the key terminology, concepts, and principles? ▪ Are they comfortable explaining concepts to others and participating in discussions? ▪ Do they generally perform independently and only seek guidance in complex or difficult situations?
Advanced	▪ Do they possess in-depth knowledge of the key terminology, concepts, and principles? ▪ Can they discuss, explain, advise, and debate concepts? ▪ Do others often seek their input and advice as a recognized expert?

Step 3: Prioritize competencies for targeted growth

Once core and technical competencies have been identified and current proficiency levels assessed, the security specialist will need to prioritize the competencies to ensure they are given the appropriate amount of attention. Here are a few considerations when prioritizing:

- The lowest proficiency levels need the most attention.
- Not all competencies carry the same weight, so target those that will currently have the biggest impact.
- If an individual is generally performing at or above target level, prioritize the competencies that will help them get to the next stage in their career, such as leadership or management competencies.
- In the early stages of a career, the security specialist may want to develop multiple competencies to help them decide the career path they want to take.

Step 4: Identify training and development opportunities

Recommended professional development training found in *Appendix D: Technical Competencies, Knowledge, Skills and Available Training* aligns to all competencies and proficiency levels discussed in this guide. Leadership programs and certifications, as well as earned credentials that validate skills and knowledge are included as well as mentoring, rotational assignments, and self-study. To help you create your development path, competencies for each opportunity are included. Review the training options individually or with a supervisor to select the best option.

Step 5: Build the Individual Development Plan (IDP)

Creating an IDP is the final step in the process. According to the Office of Personnel Management (OPM), an IDP is a tool that assists employees in career and personal development. Its primary purpose is to help employees reach short- and long-term career goals, as well as improve current job performance. An IDP is not a performance evaluation tool; it is a partnership between the employee and the supervisor that involves preparation and continuous feedback. When using an IDP, supervisors develop a better understanding of their employees' professional goals, strengths, and developmental needs. Employees take personal responsibility and accountability for their career development by acquiring and enhancing the skills they need to stay current in required skills. This living document should be reevaluated by the employee and supervisor annually to allow training and development activities to become a roadmap for future growth.

Visit the Office of Personnel Management Information to learn more about their Individual Development Plan.

Some benefits of an IDP include:

- Providing an administrative mechanism for identifying and tracking development needs and plans
- Assisting in planning for the agency's training and development requirements
- Aligning employee training and development efforts with an organization's mission, goals, and objectives[4]

There are no regulatory requirements mandating federal employees to complete IDPs. Many agencies require their employees to complete an IDP annually while other organizations only encourage its use. Further, numerous agencies have developed their own IDP planning process and forms. While there is not one "correct" form for recording an employee's development plan, an effective plan should include, at minimum, the following:

- Employee profile: Name, position title, office, grade/pay band
- Career goals: Short- and long-term goals with estimated and actual completion dates
- Development objectives: Linked to the work unit's mission, goals, and objectives and employee development needs and objectives
- Training and development opportunities: Activities the employee will pursue with estimated and actual completion dates. These activities may include formal classroom or web-based training, rotational assignments, shadowing assignments, on-the-job training, self-study programs, and professional conferences/seminars.
- Signatures: Supervisor and employee signature and date

[4] Office of Personnel Management Information on Individual Development Plan https://www.opm.gov/WIKI/training/Individual-Development-Plans.ashx

The IDP involves five phases:

1. **Pre-Planning** - Supervisor and employee prepare independently for meeting
2. **IDP Meeting** - Discussion of employee strengths, areas for improvement, interests, goals, and organizational requirements
3. **Prepare IDP** - Employee, in consultation with supervisor, completes plan for individual development
4. **Implement IDP** - Employee pursues training and development identified in plan
5. **Provide Feedback/Evaluate Outcomes** – Supervisor and employee evaluate usefulness of training and development experiences

Figure 4: IDP Process

The career progression planning process and IDPs are ultimately tools to assist employees in reaching their career goals. Advancement on a career ladder requires thoughtful consideration, planning, and communication with supervisors and mentors. Whatever process is chosen, a deliberate approach is critical to help employees focus on and enhance their competencies. The *Security Specialist Career Progression Ladder: An Interagency Security Committee Guide* can help employees chart their path to future success though it is up to each employee and supervisor to make the most of it.

Appendix A: Recommended Core Competencies

CORE COMPETENCIES	
Competency	**Description**

Accountability	• Self-accountable for measurable, high-quality, timely, cost-effective results
	• Determines objectives, sets priorities, accepts responsibility for mistakes
	• Supervisors:
	  ○ Plans, distributes, coordinates, and monitors work assignments of others
	  ○ Ensures staff are appropriately selected, utilized, developed, and treated fairly and equitably
	  ○ Manages budgeting responsibilities

Customer Service	• Communicates with customers to understand their needs • Works with customers to set expectations, keeping them informed of issues or problems • Provides timely, flexible, and responsive services to customers • Reaches out to customers to gather information about their requirements and needs • Displays flexibility in responding to changing customer needs • Independently develops creative and useful ideas that add significant value to products and services • Anticipates customer needs and resolves or avoids potential problems, maximizing customer satisfaction
Decision Making	• Makes sound, well-informed, and objective decisions • Perceives the impact and implications of decisions • Commits to action, even in uncertain situations, to accomplish organizational goals • Drives successful change
Flexibility	• Open to change and adapts work methods to unexpected obstacles
Interpersonal Skills	• Shows understanding, friendliness, courtesy, tact, empathy, concern, and politeness to others • Effectively deals with individuals who are difficult, hostile, or distressed • Relates well to people from varied backgrounds and different situations
Leadership	• Influences, motivates, and challenges others • Adapts leadership styles to a variety of situations, leads by example, guides and coaches others • Builds and maintains productive working relationships in and outside the work unit/organization • Handles conflict constructively; demonstrates initiative by taking appropriate action • Assumes personal responsibility and accountability for tasks, products, and/or services provided

CORE COMPETENCIES	
Competency	**Description**
Communication	• Effectively modifies communication style, tone, and level of specificity to the audience • Effectively explains or defends viewpoint to audiences with opposing views • Makes clear and convincing oral presentations • Listens to others and attends to nonverbal cues • Communicates in an influential or persuasive manner • Communicates clearly and concisely in writing and verbally • Applies effective listening skills and appropriately responds when communicating with others • Solicits, shows respect for, and carefully considers others' ideas, comments, and questions • Recognizes and uses correct English grammar, punctuation, and spelling • Communicates information (facts, ideas, or messages) in a succinct and organized manner • Demonstrates proficiency in Microsoft Word, PowerPoint, and Excel
Problem Solving	• Identifies problems and solutions • Uses sound judgment to generate and evaluate alternatives, and to make recommendations
Teamwork & Cooperation	• Contributes to achieving goals by working collaboratively with others and building effective partnerships across organizational boundaries • Encourages and facilitates cooperation, pride, trust, and group identity • Fosters commitment and team spirit • Works with and makes positive contributions to achieving team goals • Respects and values individual differences and perspectives by treating everyone fairly • Independently helps and provides support to advance goals • Effectively handles disagreements or conflicts, resolving them constructively • Consults with senior team members or supervisors when appropriate • Collaborates beyond what is expected resulting in high-impact contributions • Contributes to a climate of trust and skillfully develops productive relationships • Anticipates situations with potential for conflict and effectively minimizes escalation • Considers all sides of an issue and develops effective compromises or resolutions
Representing the Department or Agency	• Represents the agency and its interests in interactions with internal and external parties • Ensures interactions with outside parties reflect positively on the agency • Enhances trust and credibility in the agency and its mission • Deals professionally and tactfully with external parties in difficult or emergency situations • Acts and guides others in defusing difficult, tense, or emergency situations • Calmly and effectively manages crisis situations • Engages with others in a manner that earns their respect, advancing the goals of the agency • Accurately reads, assesses, and responds to complex organizational situations • Delivers responses in a confident and compelling manner • Handles complex and high visibility communications effectively • Tailors style and materials to communicate information effectively to different levels and types of audiences, properly emphasizing the most critical issues

SUPERVISORY CORE COMPETENCIES	
Competency	**Description**
Leading Change	• Develops and implements an organizational vision that integrates key program goals, priorities, values, and other factors; articulates the agency's vision, mission, and strategies to employees in a way that inspires their commitment; supports and manages change; responds professionally in difficult situations
Leading People	• Leads people toward meeting the organization's vision, mission, and goals; provides a workplace that fosters the development of others and facilitates cooperation and teamwork; supports constructive resolution of conflicts
Results-Driven	• Meets organizational goals and customer expectations; makes decisions that produce high-quality results by applying technical knowledge, analyzing problems, and calculating risks
Business Acumen	• Manages human, financial, and information resources strategically
Building Coalitions	• Builds coalitions internally and with other federal agencies
Assign, Monitor, and Evaluate Work	• Sets and communicates clear expectations for the work and behavior of others • Coordinates and monitors the work of others • Addresses employee performance • Identifies developmental needs and provides needed developmental or training opportunities • Effectively matches skills, availability, and experience of an individual with work assignments • Empowers staff to perform their work by providing support/guidance as needed • Effectively monitors and evaluates performance • Proactively seeks out and implements effective methods to improve unit's performance • Effectively coordinates tasks and monitors performance to exceed unit objectives • Proactively addresses difficult and potentially contentious issues regarding performance and conduct in a tactful, honest, and candid manner
Leadership	• Communicates a vision for work unit, translating broad organizational goals into concrete objectives, plans, priorities, and assignments • Maintains an awareness of external factors that affect the organization or specific work assignments • Formulates short- and long-term strategies consistent with organizational goals and other factors • Leads, develops, and manages a high performing, diverse workforce, ensuring employment practices are administered in a fair and equitable manner • Promotes a workplace where differences are valued and leveraged to achieve the vision and mission • Demonstrates an in-depth understanding of external factors that may affect the unit's work and uses this knowledge constructively in establishing goals and priorities • Creates an environment that encourages employees and stakeholders to provide input on possible enhancements or impediments to unit performance • Effectively formulates long-term strategies across organizational units that take a broad perspective and achieve significant results in support of organizational goals

Appendix B: Recommended Technical Competencies

TECHNICAL JOB COMPETENCIES (Primary and Future)	
Competency	**Description**
National/Federal Security Related Policies, Standards and Risk Management	• Implement national/federal security policies, standards, and recommendations and those established by the Interagency Security Committee (ISC) and other authorities, (National Institute of Standards & Technology (NIST) and the Office of Management and Budget (OMB); apply principles, methods, and tools used for risk assessment and mitigation, including assessment of failures and their consequences, specifically, *the Risk Management Process for Federal Facilities*: *A Interagency Security Committee Standard*, the *Active Shooter Policy and Best Practices* document, and *Prohibited Items in Federal Facilities: an ISC Standard*
Risk Assessments	• Conduct recurring risk assessments to evaluate threats, vulnerabilities, and consequences, as well as develop security countermeasures that mitigate risk to an acceptable level
Basic Security and Countermeasures	• Knowledge of how to maintain the protection of resources, encompassing loss prevention, planning, and/or programming for any new and existing facilities, equipment, and personnel • Knowledge of visitor access and control programs • Apply theory and application of protection systems, including the primary functions of detection, delay, and response and the secondary function of deterrence, including: a. Apply concepts and considerations in the integration of protection systems b. Identify applicable codes and standards pertaining to protection systems c. Understand the basic procurement process as related to security requirements d. Apply the basic concepts of project management, including project lifecycle, phases, and stakeholder management e. Read and utilize a project schedule, such as a Gantt chart or network diagram f. Test countermeasures to assure their functionality g. Read, interpret, and evaluate blueprints h. Understand electronic system communication methods, line supervision, cable types, multiplexing, network topologies, and computer peripherals i. Understand Personnel Access Control Systems (PACS), Intrusion Detection Systems (IDS), and Digital Imaging Systems (DIS)
Industrial Security	• Understand and apply security requirements as stated in EO 12829. Understand the requirements of EO 12829, as amended by EO 12885, establishing a National Industrial Security Program (NISP) to safeguard Federal Government classified information released to contractors, licensees, and grantees of the U.S. Government.
Personnel Security	• Implement suitability and national security adjudication standards to include maintaining Sensitive Compartmented Information (SCI) access.

TECHNICAL JOB COMPETENCIES (Primary and Future)	
Competency	**Description**
	• Knowledge of laws, regulations, Executive Orders, and guidance related to Federal personnel vetting, including EO 12968 and 13467, and Security Executive Agent Directives • Knowledge of Trusted Workforce 2.0 personnel vetting policies and procedures
Information Security	• Safeguard classified information, encompassing document or information classification management, release of material into the public domain, and reviews
Information Assurance, Systems and Cyber Security	• Knowledge of information assurance and methods/procedures to protect information systems, federal automated resources, and data by ensuring their availability, authentication, confidentiality, and integrity
Communications Security	• Knowledge of safeguarding COMSEC equipment in facilities
Operations Security	• Knowledge of the 5-Step OPSEC analytical process used to deny our adversaries critical information about US intentions and capabilities, (identify critical information, analyze the threat, analyze the vulnerability, assess risk, and apply countermeasures)
Counterintelligence	• Knowledge of foreign intelligence entities' tradecraft directed at DHS and the U.S. Government, including CI Motivators, CI Indicators, and the Espionage Recruitment Cycle • Knowledge, identification, and recognition of the threats of and methods used by foreign intelligence entities, including cyberattacks
Insider Threat	• Knowledge of whom is an insider, what is an insider threat, how can insider threats be expressed • Knowledge of how to establish an insider threat mitigation program • Knowledge of insider threat detection and identification
Safety, Health and Emergency Management	• Knowledge of public safety and security operations, occupational health and safety, and emergency management, preparedness, and response
Contracting Administration	• Basic understanding of the Contracting Officer's Representative (COR) duties and responsibilities as outlined within the Federal Acquisition Regulation (FAR) as found in Federal Acquisition Institute - Cornerstone OnDemand (FAI CSOD) courses

Appendix C: Competencies for Security Specialists

Competencies for security specialists can be broken into three categories: Technical, recommended core, and leadership. **Technical job competencies** encompass job duties and responsibilities that will accomplish the organization's mission and build broad-based security skills. **Recommended core competencies** reflect the critical skills that apply across all levels and positions in this occupational series, enabling you to interact with others and manage yourself as you perform your work. **Leadership competencies,** considered core for Grade Levels 9-15 or equivalent, focus on leading change, planning, strategic direction, leading people, and building coalitions in support of the mission.

Technical Job Competencies:

- Physical Security
- Industrial Security
- Personnel Security
- Information Security
- Information Assurance, Systems, and Cyber
- Communications Security
- Operations Security
- Counterintelligence
- Insider Threat
- Safety, Health, and Emergency Management
- Contracting Administration

Recommended Core Competencies:

- Accountability and Management
- Customer Service
- Decision Making
- Flexibility
- Interpersonal Skills
- Leadership
- Oral Communication
- Problem Solving
- Teamwork
- Written Communication and Writing

Leadership Competencies (core for Grade Levels 9-15 or equivalent)**:**

- Leading Change
- Leading People
- Results-Driven
- Business Acumen
- Building Coalitions

Appendix D: Technical Competencies, Knowledge, Skills and Available Training

In today's training and educational environment, there are numerous courses, webinars, self-directed and formal educational courses available in-person and online for developing desired competencies. Employees should check with their department or agency for in-house training before seeking outside training.

Training courses for the desired knowledge, skills, and recommended for each competency are listed below. Please visit the recommended training course links for detailed course descriptions and prerequisites. Additionally, contact the vendors to check course availability, location, and cost. The recommended training courses serve as an example of a typical training program. Any training/development plan should be tailored to suit the agency's mission and the uniqueness of the security position.

SECURITY SPECIALIST COMPETENCIES:

D.1 PHYSICAL SECURITY

D.1.1 Desired Knowledge, Skills, and Understanding

- Describe the national and federal security policy standards, including those established by the Interagency Security Committee (ISC) and other security authorities.
- Cite the principles, methods, and tools used for risk assessment and mitigation.
- Articulate the mission of the ISC.
- Understand the policy and procedures used by a Facility Security Committee (FSC) when presented with security issues, and the roles and responsibilities of the committee members.
- Define the criteria and successfully utilize the process for determining a Facility Security Level (FSL).
- Identify the steps of the "ISC Risk Management Process" for federal buildings and facilities in the U.S. occupied by federal employees for nonmilitary activities.
- Define and successfully utilize the process for determining security criteria and the customized security measures required at a specific federal facility.
- Articulate the Crime Prevention Through Environmental Design (CPTED) principles and how they may be implemented in the design of an effective interior and exterior building environment to reduce the fear of potential crime and terrorist activity and encourage desirable behavior.
- Describe the concept of critical infrastructure under the National Infrastructure Protection Plan (NIPP) and the need to adequately protect such facilities and assets.
- Explain National Fire Protection Association (NFPA) and emergency management codes, (101: Life Safety Code), that address construction, protection, and occupancy features necessary to minimize danger to life from the effects of fire, (smoke, heat, and toxic gases).
- Explain how to conduct recurring security assessments to evaluate threats, vulnerabilities, and impact of loss/consequences, as well as develop security countermeasures that mitigate risk to an acceptable level.

- Demonstrate all components of a security assessment including research; inspection; threat assessment; countermeasure approval process and ISC/FSC policies; documentation and reporting of key findings and recommendations; presentation of findings.
- Conduct market survey/pre-lease, new construction, and special assessments, demonstrating a general understanding of new site drawings/maps.
- Articulate how to maintain the protection of resources through loss prevention, planning, and/or programming for any new and existing facilities, equipment and personnel, and administration of the Visit Control Program.
- Oversee security of facilities including access control systems; security design and engineering; video monitoring; alarm system design and installation; emergency response plans and procedures; mail screening equipment and procedures; biometrics; protective lighting; storage/safes; security locks/locking devices; crime prevention and security awareness; security force specification and management.
- Identify additional security-related tasks including coordinating law enforcement liaison activities; performing guard operations (communications, patrol routes, firearms training, reporting procedures, K- 9 ops); managing special security areas (locks and alarms); coordinating anti-terrorism activities (back-up forces, roadblocks, barriers); writing security policy and procedures manuals. protection system elements; codes and standards pertaining to protection systems; basic concepts of the procurement process as related to security requirements and enhancements.
- Testing countermeasures to assure their functionality; electronic system communication methods, line supervision, cable types, multiplexing, network topologies, and computer peripherals; concepts of alarm communication and display and the different technologies available; intrusion detection system performance characteristics (probability of detection, nuisance alarm rate, and vulnerability to defeat); identifying the differences between active and passive sensors, overt and covert sensors, and volumetric and line detection sensors; identifying discrepancies in line supervision by inspecting sensor and control panel terminations; using standards from the American National Standards Institute and Underwriters Laboratory for Intrusion Detection Systems.

D.1.2 Recommended Training Courses

Defense Counterintelligence and Security Agency (DCSA): Center for Development of Security Agency (CDSE)

- Introduction to Physical Security
- Physical Security Measures
- Physical Security Planning and Implementation
- Applying Physical Security Concepts*
- Lock and Key Systems
- Storage Containers and Facilities
- Exterior Security Lighting
- Electronic Security Systems
- Antiterrorism Officer (ATO) Level II
- Physical Security Virtual Environment Assessment*

Interagency Security Committee (ISC) courses provided by Federal Emergency Management Agency (FEMA): Emergency Management Institute (EMI)

- IS-1170 – Introduction to the Interagency Security Committee (ISC)
- IS-1171 – Overview of Interagency Security Committee (ISC) Publications
- IS-1172 – Risk Management Process for Federal Facilities - Facility Security Level (FSL) Determination
- IS-1173 – Levels of Protection (LOP) and Application of the Design-Basis Threat (DBT) Report (U)
- IS-1174 – Facility Security Committees (FSCs)
- Active Shooter: What you can do
- Active Shooter Prevention
- Workplace Security Awareness (FEMA)
- Critical Infrastructure Security: Theft and Diversion - What You Can Do (FEMA)
- The National Infrastructure Protection Plan, An Introduction

ISC courses provided by OPM

- Federal Risk Management Process Training Program

CISA

- Active Shooter Preparedness Webinar (CISA)

D.2. INDUSTRIAL SECURITY

D.2.1 Desired Knowledge, Skills, and Understanding

- Describe security requirements as stated in the National Industrial Security Program Operating Manual (NISPOM).
- Articulate the requirements of 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.
- Demonstrate competence in the execution of all security requirements of the NISP Operating Manual including waivers and exceptions to this manual.
- Apply knowledge of industrial, personnel, IT, and information security policies and procedures, federal contracting laws and regulations, and facility clearances.
- Identify methods to mitigate foreign ownership, control, and influence, and understand the structure of the Committee on Foreign Investments in the U.S.

D.2.2 Recommended Training Courses

CDSE

- Introduction to Industrial Security
- Industrial Security Basics
- Getting Started Seminar for New FSOs*
- Business Structures in the National Security Program (NISP)

- Clearances in Industrial Security: Putting it All Together
- DCSA Security Rating Criteria Requirements
- Facility Clearances in the NISP
- Personnel Clearances in the NISP
- Safeguarding Classified Information in the NISP

D.3 PERSONNEL SECURITY

D.3.1 Desired Knowledge, Skills, and Understanding

- Implement the Personnel Security Program, including the criteria for adjudicating personnel security clearances and how to maintain Sensitive Compartmented Information (SCI).
- Articulate the requirements of all personnel and national security executive orders and directives.
- Develop and execute 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 (SAP), and reinvestigation; sensitive and public trust positions; interviews and due process; authority to waive investigative requirements; reciprocity of prior investigations and personnel security determinations; procedures for appeals of security clearance denials and revocations.

D.3.2 Recommended Training Courses

CDSC

- Introduction to Personnel Security
- Introduction to Special Access Programs (SAP)
- SAP Mid-Level Security Management

OPM

- Central Verification System
- Position Designation

D.4 INFORMATION SECURITY

D.4.1 Desired Knowledge, Skills, and Understanding

- Describe how to safeguard classified information, encompassing document or information classification management, release of material into the public domain, and classification/declassification reviews.
- Explain all requirements for classifying, safeguarding, and declassifying national security information, including original classification; derivative classification; declassification and downgrading; safeguarding; implementation and review; and general provisions.

- Conduct compliance inspections and unauthorized disclosure investigations.
- Summarize the requirements and mandates for identifying, safeguarding, controlling, destroying, and storing of Personally Identifiable Information (PII), and the reporting procedures for loss or theft of PII.

D.4.2 Recommended Training Courses

CDSE

- Introduction to Information Security
- Information Security Management*
- Information Security Emergency Planning
- Identifying and Safeguarding Personally Identifiable Information (PII)
- Original Classification
- Security Classification Guidance
- Marking Classified Information
- Classification Conflicts and Evaluations
- Derivative Classification
- Derivative Classification Refresher
- Unauthorized Disclosure of Classified Information for DoD and Industry
- Unauthorized Disclosure Refresher

D.5 INFORMATION ASSURANCE, SYSTEMS AND CYBERSECURITY

D.5.1 Desired Knowledge, Skills, and Understanding

- Explain information assurance and the methods and procedures to protect information systems, federal automated resources, and data by ensuring their availability, authentication, confidentiality, and integrity.
- Demonstrate and exercise a functional awareness of the threats, vulnerabilities, and security requirements of information systems towards the enterprise security profile design, to include: information systems security and the electronic access control system (EPACS); information technology (IT)-based vulnerabilities and inherent threats posed to the enterprise security system (ESS) when connected to a networked IT system; security countermeasures to reduce Information Security and IT- based threats and vulnerabilities towards the ESS/EPACS; IT security architecture and design (firewalls, intrusion detection systems [IDS], virtual private networking, and virus protection technologies).
- 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.
- Articulate the NIST Risk Management Framework (RMF) and the processes used to assess information technology systems and equipment.
- Describe NIST Security Standards and Guidelines and Federal Information Processing Standard (FIPS) 200.
- Demonstrate knowledge and understanding of the Committee on National Security Systems policies and procedures.
- Explain PIV credentials defined by the NIST and FIPS 201 as an end- point PIV Card.

- Outline the requirements of various access control systems ("off the shelf") that are approved for use under HSPD- 12, FIPS 201.
- Describe the architecture of an enterprise system following the recommendations in the NIST SP 800-116 document.

D.5.2 Recommended Training Courses

National Institute of Standards & Technology (NIST)

- NIST Risk Management Framework Training

The Office of the Director of National Intelligence (ODNI)

- Cybersecurity Training Series (ODNI)

CDSE

- Introduction to the Risk Management Framework
- Risk Management Framework (RMF) Step 1: Categorization of the System
- Risk Management Framework (RMF) Step 2: Selecting Security Controls
- Risk Management Framework (RMF) Step 3: Implementing Security Controls
- Risk Management Framework (RMF) Step 4: Assessing Security Controls
- Risk Management Framework (RMF) Step 5: Authorizing Systems
- Risk Management Framework (RMF) Step 6: Monitor Security Controls
- Cybersecurity Awareness
- Cyber Awareness Challenge for the Intelligence Community
- Phishing Awareness

D.6 COMMUNICATIONS SECURITY

D.6.1 Desired Knowledge, Skills and Understanding

- Explain how to implement, develop, and maintain a Communications Security Program and control cryptographic equipment.
- Describe how secure communications are controlled and managed across the nation under a separate set of National Security Agency (NSA) Central Security Service standards and procedures.
- Successfully complete the certified COMSEC Custodian course recognized by the NSA.
- Articulate the duties of a COMSEC Custodian: identifying, controlling/storing, and handling COMSEC material; reporting COMSEC incidents; completing COMSEC forms; ordering COMSEC material/equipment; destruction procedures for COMSEC material/equipment.

D.6.2 Recommended Training Courses

National Security Agency (NSA)

- *COMSEC Custodian Training (directly through NSA only)*

D.7 OPERATIONS SECURITY

D.7.1 Desired Knowledge, Skills, and Understanding

- Describe critical technologies, foreign intelligence collection systems and techniques, and security countermeasures.
- Explain purpose of OPSEC surveys and Protection Assessment Reviews (PARs).
- 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".
- Outline the five-step Operations Security Process: 1. Identification of critical information; 2. Analysis of threats; 3. Analysis of vulnerabilities; 4. Assessment of risk; and 5. Application of appropriate OPSEC measures.
- Demonstrate a working knowledge of an OPSEC program including assigning responsibility for OPSEC direction and implementation; planning for and implementing OPSEC in anticipation of and, where appropriate, during department activity; using OPSEC analytical techniques to assist in identifying vulnerabilities and to select appropriate OPSEC measures; enacting 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 to improve OPSEC programs; providing interagency support and cooperation with respect to OPSEC programs

D.7.2 Recommended Training Courses

CDSE

- OPSEC Awareness
- Introduction to Risk Management
- Critical Thinking for Insider Threat
- Counterintelligence Awareness and Reporting (CDSE)

National Archives

- Unauthorized Disclosure: Preventing and Reporting
- CUI Program Overview

Office of the Director of National Intelligence

- OPSEC For All (ODNI)
- OPSEC Analysis: In-Person (ODNI)
- OPSEC Program Management In-Person (ODNI)

FEMA

- Surveillance Awareness: What You Can Do (FEMA)

D.8 COUNTERINTELLIGENCE AND INSIDER THREAT

D.8.1 Desired Knowledge, Skills and Understanding

- Identify the threats and methods of foreign intelligence entities and recognition of foreign intelligence entities' use of cyber-attacks.
- Articulate how to identify the role of threat awareness in protecting the national industrial base; foreign collection attempts targeting U.S. critical technologies; key types of threats and common methods of operation; information most likely to be targeted by espionage; types of suspicious events and behaviors that should be reported and how to report them.

D.8.2 Recommended Training Courses

CISA

- Understanding the Insider Threat (CISA Video)

CDSE

- Thwarting the Enemy: Providing Counterintelligence & Threat Awareness to the Defense Industrial Base
- Critical Thinking for Insider Threat
- Insider Threat Awareness
- Counterintelligence Awareness and Reporting for DOD

FEMA

- IS-915 Protecting Critical Infrastructure Against Insider Threats

D.9 SAFETY, HEALTH, AND EMERGENCY MANAGEMENT

D.9.1 Desired Knowledge, Skills, and Understanding

- Describe public safety and security operations, occupational health and safety, and emergency management, preparedness, and response.
- Define the requirements of National Security Presidential Directive- 51, Homeland Security Presidential Directive (HSPD)- 20, and/or other pertinent policies regarding Continuity of Operations (COOP).
- Develop a basic COOP plan and understand COOP reporting and national level exercise requirement.
- Articulate pertinent federal management regulations and department or agency specific policies regarding the Occupant Emergency Program (OEP)
- Develop an All-Hazards OEP, including evacuation and shelter-in-place plans
- Test and evaluate an OEP, making appropriate modifications as necessary.
- Describe the operating requirements and components for an Incident Command System (ICS) for managing short-term and long-term field operations for a broad spectrum of emergencies
- Identify 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.
- Explain the formation and structure of federal response organizations and how they interface with local emergency response organizations in an emergency incident.

- Describe approved personal protective equipment, especially respiratory protective equipment including the National Institute of Occupational Safety and Health (NIOSH) Certification List, and protective measures when administering first aid; the latest Federal Pandemic Influenza Plan Federal Pandemic Influenza Plan; The NIOSH Pocket Guide to Chemical Hazards (Current Edition) available both in hardcopy and on-line at National Institute for Occupational Safety & Health | NIOSH | CDC.

D.9.2 Recommended Training Courses

FEMA EMI

- Continuity of Operations (COOP) Awareness Course
- Introduction to Continuity of Operations (COOP)*
- Introduction to Incident Command System (ICS)
- Introduction to National Incident Management (NIMS)
- A National Response Framework (NRF), An Introduction
- Fundamentals of Emergency Management*
- Planning: Emergency Operations
- Introduction to COOP Planning for Pandemic Influenzas
- Exercising COOP Plans for Pandemics Course
- Incident Command System (ICS) for Single Resources and Initial Action Incidents*

Additional training can be found on FEMA's EMI website or within FEMA's broader National Training and Education (NTE) Course Catalog.

Occupational Safety and Health Administration (OHSA)

- Occupational Safety and Health Course for Other Federal Agencies

Center for Disease Control (CDC)/National Institute of Occupational Safety and Health (NIOSH) Training

- Assorted CDC/NIOSH Training Courses
- Assorted CDC/NIOSH Chemical Safety Courses & Resources

D.10 CONTRACTING ADMINISTRATION

D.10.1 Desired Knowledge, Skills and Understanding

- Articulate the Contracting Officer Representative's (COR) duties and responsibilities as outlined within FAITAS and requirements.
- Explain the facility clearance approval process and the requirements for making a Foreign Ownership, Control, or Influence determination for contractors.
- Work with contracting staff on monitoring various types of contracts such as guard service, construction, countermeasure implementation, etc.
- Prepare statements of work, limited source justifications, and acquisition plans after completion of formal training and detail assignment in the contracting office.
- Describe the basic elements of an access control system, how to specify a system, and understand the concept of "defense in depth".
- Learn how to commission and closeout projects.

D.10.2 Recommended Training Courses

CDSE

- Acquisitions and Contracting Basics in the National Industrial Security Program (NISP) IS123.16 (cdse.edu)

Federal Acquisition Institute (FAI)

- FAI Training Application Service (FAITAS) Courses
- FAI Ongoing Lunch Training Seminars

D.11 ACCOUNTABILITY AND MANAGEMENT

D.11.1 Desired Knowledge, Skills and Understanding

- Hold self and others accountable for measurable, high-quality, timely, and cost-effective results; determine objectives, set priorities, and delegate work; accept responsibility for mistakes; comply with established control systems and rules; plan, distribute, coordinate, and monitor work assignments of others; evaluate and provide performance feedback; ensure staff are appropriately selected, utilized, and developed, and treated fairly and equitably; manage budgeting responsibilities, if applicable.

D.11.2 Recommended Training Courses

OPM Center for Leadership Development

- Supervisory Development I: Fundamentals
- Supervisory Development II: Learning to Lead
- Management Development: Leading from the Middle
- Project Management Principles

D.12 CUSTOMER SERVICE

D.12.1 Desired Knowledge, Skills and Understanding

- Work with all individuals who use or receive the services or products the work unit produces, (the public, individuals who work in Office of Security [OSY], other offices/departments, or organizations outside the government) to assess their needs; provide information or assistance; resolve problems or satisfy their expectations; identify available products and services; and provide quality products and services.

D.12.2 Recommended Training Courses

FEMA

- Introduction to Public-Private Partnerships
- Effective Communication

D.13 DECISION MAKING

D.13.1 Desired Knowledge, Skills and Understanding

- Make sound, well-informed, and objective decisions; perceive the impact and implications of decision; commit to action, even in uncertain situations, to accomplish organizational goals; drive successful change.

D.13.2 Recommended Training Courses

FEMA

- Decision Making and Problem Solving

D.14 FLEXIBILITY

D.14.1 Desired Knowledge, Skills and Understanding

- Remain open to change and new information; adapt behavior or work methods in response to new information, changing conditions, or unexpected obstacles; effectively deal with ambiguity.

D.14.2 Recommended Training Courses

OPM Center for Leadership Development

- Managing the Flexible Workplace

D.15 INTERPERSONAL SKILLS

D.15.1 Desired Knowledge, Skills and Understanding

- Demonstrate understanding, friendliness, courtesy, tact, empathy, concern, and politeness to others; develop and maintain effective relationships with others; effectively deal with individuals who are difficult, hostile, or distressed.

D.15.2 Recommended Training Courses

Check Your Department or Agency Related Training

D.16 LEADERSHIP

D.16.1 Desired Knowledge, Skills and Understanding

- Influence, motivate, and challenge others; adapt leadership styles to a variety of situations and lead by example, including: guiding, coaching, and/or mentoring others; building and maintaining productive working relationships within and outside the work unit/organization; handling conflict constructively; demonstrating initiative by taking appropriate action without being directed to do so and influencing others in work unit to accomplish responsibilities; assuming personal responsibility and accountability for tasks, products, and/or services provided.

D.16.2 Recommended Training Courses

OPM Center for Leadership Development

- Leadership Competencies: Preparing for the Next Step

FEMA

- Leadership and Influence

D.17 COMMUNICATION

D.17.1 Desired Knowledge, Skills and Understanding

- Effectively express information to individuals or groups, considering the audience and nature of the information, (technical, sensitive, controversial); make clear and convincing oral presentations; listen to others, attend to nonverbal cues, and respond appropriately.

D.17.2 Recommended Training Courses

OPM Center for Leadership Development

- Communicating Face to Face

FEMA

- Effective Communication (FEMA)

D.18 PROBLEM SOLVING

D.18.1 Desired Knowledge, Skills and Understanding

- Identify problems; determine accuracy and relevance of information; use sound judgment to generate and evaluate alternatives, and to make recommendations.

D.18.2 Recommended Training Courses

FEMA

- Decision Making and Problem Solving

D.19 TEAMWORK

D.19.1 Desired Knowledge, Skills and Understanding

- Encourage and facilitate cooperation, pride, trust, and group identity; foster commitment and team spirit; work with others to achieve goals.

D.19.2 Recommended Training Courses

OPM Center for Leadership Development

- Team Building and Team Leadership

D.20 WRITTEN COMMUNICATION AND WRITING

D.20.1 Desired Knowledge, Skills and Understanding

- Recognize and apply correct English grammar, punctuation, and spelling; communicate information, (facts, ideas, or messages), in a succinct and organized manner; produce written information, which may include technical material that is appropriate for the intended audience; demonstrate proficiency in Microsoft Office Suite, including Word, PowerPoint, and Excel.

D.20.2 Recommended Training Courses

OPM Center for Leadership Development

- Effective Writing in Federal Government

LEADERSHIP COMPETENCIES:

D.21 LEADING CHANGE - EXECUTIVE CORE QUALIFICATION #1

D.21.1 Desired Knowledge, Skills and Understanding

- Develop and implement an organizational vision that integrates key program goals, priorities, values, and other factors; articulate OSY's vision, mission, and strategies to employees in a way that inspires commitment; support and manage change; respond professionally in stressful and difficult situations; improve effectiveness by creating an environment that rewards creativity and innovation.
- **Creativity & Innovation:** Develop new insights into situations; question conventional approaches; encourage new ideas and innovations; design and implement new or cutting-edge programs and processes.
- **External Awareness:** Understand and stay current on local, national, and international policies and trends affecting the organization and shaping stakeholders' views; be aware of the organization's impact on the external environment.
- **Flexibility:** Remain open to change and new information; rapidly adapt to new information, changing conditions, or unexpected obstacles
- **Resilience:** Effectively deal with pressure; remain optimistic and persistent, even under adversity; recover quickly from setbacks.
- **Strategic Thinking:** Formulate objectives and priorities; implement plans consistent with the long-term interests of the organization in a global environment; capitalize on opportunities and manages risks.
- **Vision**: Take a long-term view and build shared vision with others; drive organizational change; influence others to translate vision to action.

D.21.2 Recommended Training Courses

OPM Center for Leadership Development

- Strategic Planning for Executives
- Executive Development - Leading Change*
- Adapting to Organizational Change - Enabling 21st Century Leaders
- Executive Communication Skills: Leading the Process of Change
- Organizational Resiliency
- Resiliency 2.0

D.22 LEADING PEOPLE - EXECUTIVE CORE QUALIFICATION #2

D.22.1 Desired Knowledge, Skills and Understanding

- **Creativity & Innovation:** Develop new insights into situations; question conventional approaches; encourage new ideas and innovations; design and implement new or cutting-edge programs and processes.
- **External Awareness:** Understand and stay current on local, national, and international policies and trends that affect the organization and shape stakeholders' views; aware of the organization's impact on the external environment.
- **Flexibility:** Remain open to change and new information; rapidly adapt to new information, changing conditions, or unexpected obstacles.
- **Resilience:** Effectively deal with pressure; remain optimistic and persistent, even under adversity; recover quickly from setbacks.
- **Strategic Thinking:** Formulate objectives and priorities; implement plans consistent with the long-term interests of the organization in a global environment; capitalize on opportunities and manages risks.
- **Vision**: Take a long-term view and build shared vision with others; drive organizational change; influence others to translate vision to action.
- **Conflict Management:** Encourage creative tension and differences of opinions; anticipate and take steps to prevent counter-productive confrontations; manage and resolve conflicts and disagreements in a constructive manner.
- **Leveraging Diversity:** Foster a workplace where individual differences are valued and leveraged to achieve the vision and mission of the organization.
- **Developing Others:** Develop the ability of others to perform and contribute to the organization by providing ongoing feedback and opportunities to learn through formal and informal methods.
- **Team Building:** Inspire and foster team commitment, spirit, pride, and trust; facilitate cooperation and motivate team members to accomplish group goals.

D.22.2 Recommended Training Courses

OPM Center for Leadership Development

- Collaborative Leadership: Working with Others
- Engaging and Encouraging Employees
- Facilitation Skills for Leaders
- Coaching and Mentoring for Excellence

D.23 RESULTS-DRIVEN - EXECUTIVE CORE QUALIFICATION #4

D.23.1 Desired Knowledge, Skills and Understanding

- Meet organizational goals and customer expectations; make decisions that produce high-quality results by applying technical knowledge, analyzing problems, and calculating risks.
- **Accountability:** Hold self and others accountable for measurable, high- quality, timely, and cost-effective results; determine objectives, set priorities, delegate work; accept responsibility for mistakes; comply with established control systems and rules.
- **Customer Service:** Anticipate and meet the needs of both internal and external customers; deliver high-quality products and services.
  commit to continuous improvement.
- **Decisiveness:** Make well-informed, effective, and timely decisions, even when data are limited, or solutions produce unpleasant consequences; perceive the impact and implications of decisions.
- **Entrepreneurship:** Position the organization for future success by identifying new opportunities; build the organization by developing or improving products or services; take calculated risks to accomplish organizational objectives.
- **Problem Solving:** Identify and analyze problems; weigh relevance and accuracy of information; generate and evaluate alternative solutions; make recommendations.
- **Technical Credibility:** Understand and apply principles, procedures, requirements, regulations, and policies related to specialized expertise.

D.23.2 Recommended Training Courses

OPM Center for Leadership Development

- Developing Customer-Focused Organizations
- Creating and Sustaining Organizational Excellence
- Extraordinary Leadership

D.24 BUSINESS INSIGHT - EXECUTIVE CORE QUALIFICATION #5

D.24.1 Desired Knowledge, Skills and Understanding

- Manage human, financial, and information resources strategically.
- **Financial Management:** Understand OSY's financial processes; prepare, justify, and administer program budget; oversee procurement and contracting to achieve desired results; monitor expenditures and use cost-benefit mindset to set priorities.
- **Human Capital Management:** Build and manage workforce based on organizational goals, budget considerations, and staffing needs; ensure employees are appropriately recruited, selected, appraised, and rewarded; address performance problems; manage a multi-sector workforce and a variety of work situations.
- **Technology Management:** Be aware of current technological developments; make effective use of technology to achieve results; ensure access to and security of technology systems.

D.24.2 Recommended Training Courses

OPM Center for Leadership Development

- Management Development: Leading Organizations

D.25 BUILDING COALITIONS - EXECUTIVE CORE QUALIFICATION #6

D.25.1 Desired Knowledge, Skills and Understanding

- Build coalitions internally and with other federal agencies, state and local governments, nonprofit and private sector organizations, foreign governments, or international organizations to achieve common goals.

D.25.2 Recommended Training Courses

ManagementConcepts.com

- Influencing Skills
- Negotiation Skills

OPM Center for Leadership Development

- Inter-Organizational Collaboration
- Leadership for a Global Society
- Working with Congress for Federal Executives
- Science, Technology, and Public Policy
- National Security Policy
- Conflict and Negotiations for Federal Executives

Appendix E: Resources

Supervisors and employees work together to complete the employee's development plan; however, employees are ultimately responsible for taking the initiative in their professional development. Below are examples of activities one may incorporate into their plan for further development:

- **Formal Training** - OPM offers formal training at its Management Development Centers and Federal Executive Institute. There are also other formal training centers available to employees outside OPM.
- **360 Degree Feedback** - 360-degree feedback is a widely used method and tool to assist in identifying strengths and developmental needs. OPM offers 360-degree survey services as do other organizations.
- **Mentoring and Coaching** - Mentoring and coaching are effective tools for personal and leadership development. For more information, go to our Mentoring-and-Coaching.
- **Rotational/Detail Assignments** - Employees may have the option to participate in detailed, special/short-term assignments and projects, and to engage in other creative ways that expand their capacity to serve.

Organizations with IDP Programs/Templates

Below is a list of agencies that have implemented an IDP program and/or template. Several agencies also have individual development planning and career management programs in place. Please note that OPM does not endorse any format. The information below is for illustrative purposes only.

IDP Templates:

- U.S. Department of Justice - LEAP
- U.S. Department of Labor
- U.S. Environmental Protection Agency
- U.S. Department of Navy
- U.S. Small Business Administration
- U.S. Department of Education
- U.S. Department of Treasury

Organizations who provide resources and training to develop an IDP:

- U.S. Small Business Administration, Office of Disaster Assistance, IDP Guidebook
- Center for Disease Control Fact Sheet
- MIT Career Development Guide
- Smithsonian PowerPoint Presentation
- Department of Justice IDP Briefing
- U.S. Fish and Wildlife Service offers an online course
- Department of Homeland Security Career Path (only available to DHS employees)

Other helpful tips and resources

- GovLeaders.org article, *Using IDPs to Leverage Strengths*
- Career Advancement: Federal Employees Career Development Center

Appendix E.1 Glossary

TERM	DEFINITION
Competencies	A combination of the knowledge, skills, abilities, and behaviors that are needed to be successful in a job.
Facility Security Committee (FSC)	A committee that is responsible for addressing facility-specific security issues and approving the implementation of security measures and practices in multi-tenant facilities. Formerly known as the Building Security Committee (BSC), the FSC consists of representatives of all federal tenants in the facility, the security organization, and the owning or leasing department or agency. In the case of new construction or pending lease actions, the FSC will also include the project team and the planned tenant(s).
Individual Development Plan (IDP)	A tool to assist employees in career and personal development. Its primary purpose is to help employees reach short and long-term career goals, as well as improve current job performance.
Proficiency	The level or degree of competence or skill; expertise.
Professional development	The process of identifying goals and learning new skills to grow and succeed at work.

Appendix E.2 Acronyms

ATO	Antiterrorism Officer
CDC	Center for Disease Control
CDSE	Center for Development of Security Excellence
CI	Counterintelligence
COMSEC	Communications Security
COOP	Continuity of Operations
COR	Contracting Officer's Representative
CPTED	Crime Prevention Through Environmental Design
CSOD	Cornerstone On-Demand
DAU	Defense Acquisition University
DBT	Design-Basis Threat
DCSA	Defense Counterintelligence and Security Agency
DHS	Department of Homeland Security
DIS	Digital Imaging Systems
DOD	Department of Defense
EMI	Emergency Management Institute
E.O.	Executive Order
EPACS	Electronic Personnel Access Control System
ESS	Enterprise Security System
FAI	Federal Acquisition Institute
FAITAS	Federal Acquisition Institute Training Application Service
FAR	Federal Acquisition Regulation
FEMA	Federal Emergency Management Institute
FIPS	Federal Information Processing Standard
FOUO	For Official Use Only
FSC	Facility Security Committee
FSL	Facility Security Level
GSA	General Services Administration
HSPD	Homeland Security Presidential Directive
ICS	Incident Command System
IDP	Individual Development Plan
IDS	Intrusion Detection Systems
ISC	Interagency Security Committee
IT	Information Technology
LEAP	Leadership Excellence and Achievement program
LOP	Level of Protection
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
NISPOM	National Industrial Security Program Operating Manual
NIST	National Institute of Standards and Technology
NSA	National Security Agency

NTE	National Training and Education
OEP	Occupant Emergency Program
OMB	Office of Management and Budget
OPM	Office of Personnel Management
OPSEC	Operations Security
OSY	Office of Security
PACS	Personnel Access Control System
PARS	Protection Assessment Reviews
PII	Personally Identifiable Information
PIV	Personal Identity Verification
RMF	Risk Management Framework
RMP	Risk Management Process
SAP	Special Access Programs
SCI	Sensitive Compartmented Information

Appendix E.3 References

Executive Order 12829 – National Industrial Security Program, January 6, 1993

Executive Order 12885 – Amendment to Executive Order No. 12829, December 14, 1993

Executive Order 12977 – Interagency Security Committee, October 24, 1995

Executive Order 14111 – Interagency Security Committee, November 27, 2023

Executive Order 13434 - *National Security Professional Development, May 17, 2007*

Federal Acquisition Regulation (FAR)

The Risk Management Process: An Interagency Security Committee Standard

Items Prohibited in Federal Facilities: An Interagency Security Committee Standard

Planning and Response to an Active Shooter: An Interagency Security Committee Policy and Best Practices

Security Specialist Competencies: An Interagency Security Committee Guide, January 2017, 2nd Edition

Acknowledgments

The ISC would like to thank the participants of the ***Training Subcommittee.***

Training Subcommittee

Bernard Holt, Chair,
Deputy Chief, ISC

Subcommittee Members

Jeff Britton
Internal Revenue Service

Jon C. Clark
Defense Counterintelligence and Security Agency

Richard Dine
National Archives and Records Administration

Jennie Dingman
Federal Protective Service

Joshua Ederheimer
Federal Protective Service

Michael Fluck
Internal Revenue Service

Antonio Gallegos
Defense Counterintelligence and Security Agency

Michael Griffin
General Services Administration

Raymond Hankins
National Labor Relations Board

Casandra Isbell
Federal Protective Service

Kevin McCombs
Office of Personnel Management

Mackenzie McGuire
Department of Commerce

Daniel McKenna
Federal Protective Service

Rachel Meredith
Federal Bureau of Investigation

Mark McQuait
Pentagon Force Protection Agency

Dennis Ouellette
Internal Revenue Service

Ivan Pabon
Federal Protective Service

Nina Park
Federal Protective Service

John Rossiter
Securities and Exchange Commission

Gregory Shepard
Pentagon Force Protection Agency

Jerry Stanphill
Federal Aviation Administration Agency

Darryl Wortman
Department of Homeland Security

Interagency Security Committee

Daryle Hernandez, Chief

Malcolm "Dwayne" Parrish
Training Subcommittee Facilitator

Glenn Panaro
Training Subcommittee Facilitator

Scott Dunford
Senior Security Specialist

Jami Craig
Technical Editor