UNITED STATES OFFICE OF PERSONNEL MANAGEMENT

# Interpretive Guidance for Cybersecurity Positions

## Attracting, Hiring and Retaining a Federal Cybersecurity Workforce


**OPM**.GOV

OCTOBER **2018**

# THE U.S. OFFICE OF PERSONNEL MANAGEMENT INTERPRETIVE GUIDANCE FOR CYBERSECURITY POSITIONS

## ATTRACTING, HIRING AND RETAINING A FEDERAL CYBERSECURITY WORKFORCE


EMPLOYEE SERVICES
CLASSIFICATION AND ASSESSMENT POLICY
TALENT ACQUISITION AND WORKFORCE SHAPING
U.S. OFFICE OF PERSONNEL MANAGEMENT



OCTOBER 11, 2018



FEDCLASS@OPM.GOV
202-606-3600

## Table of Contents

# Introduction

The U.S. Office of Personnel Management (OPM) is issuing this policy guidance for cybersecurity positions to help agencies attract, hire, and retain a highly skilled cybersecurity workforce. This interpretive guidance addresses position classification, job evaluation, qualifications and assessment for cybersecurity positions. OPM is issuing this guidance to assist agencies as they:

- Identify cybersecurity positions;
- Clarify cybersecurity roles and duties;
- Address position management issues;
- Recruit, hire, and develop a qualified cybersecurity workforce to meet their agency needs;
- Implement training, performance, and retention programs; and
- Conduct cybersecurity workforce assessments.

OPM has worked with lead agencies and other Federal stakeholders to gain a better understanding of the cybersecurity workforce Governmentwide. OPM gained insight and feedback from key agencies and other stakeholders with cybersecurity functions to include: representatives from OPM, the Office of Management and Budget (OMB), the Chief Human Capital Officers (CHCO) Council, the Chief Information Officer Council (CIOC), and Department of Commerce's National Institute of Standards and Technology (NIST) in coordination with the Department of Homeland Security (DHS), Department of Defense (DOD), and other stakeholder groups.

This guidance supports the President's Management Agenda (PMA): Modernizing Government for the 21st Century which was released March 20, 2018, and emphasizes reducing Cybersecurity risks to the Federal mission by leveraging current commercial capabilities and implementing cutting edge cybersecurity capabilities and building a modern IT workforce by recruiting, reskilling, retaining professionals able to help drive modernization with up-to-date technology. This guidance also supports EO 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, dated 05/11/2017, which highlights workforce development to ensure that the United States maintains a long-term cybersecurity advantage.

The next section will provide background and overview of the work performed by OPM and others related to cybersecurity over the years.

# BACKGROUND

## Cybersecurity in the Federal Government

The nature and scope of cybersecurity work is constantly evolving. Many efforts have been undertaken to identify the cybersecurity workforce within the Federal Government. Below is a

sample of some of the important directives/guidance addressing the Federal Cybersecurity workforce, which also informed OPM's efforts to identify cybersecurity work.

| DIRECTIVE/MODEL | DESCRIPTION | RELEASE DATE |
|---|---|---|
| **DOD Directive 8570 – Information Assurance Training, Certification, and Workforce Management (See DOD Directive 8140.01 below)** | • Provided the basis for agency-wide solution to train, qualify, and manage the DOD Information Assurance (IA) workforce.<br>• Divided IA field into two areas: technical and management.<br>• Directive was reissued and renumbered in August 2015 with DOD Directive 8140. | August 2004 |
| **DOD Directive 8570.01-M – Information Assurance Workforce Improvement Program** | • Companion to the original directive 8570.<br>• Divided the DOD IA workforce into six defined categories and specified certification requirements. | December 2005<br>Revised November 2015 |
| **NIST SP 800-100 – Information Security Handbook: A Guide for Managers** | • Identified 13 areas of information security management. | October 2006 |
| **OPM Federal Cybersecurity Competency Model** | • Identified core competencies and tasks critical to the Federal Cybersecurity workforce. | February 2011 |
| **DHS Advisory Council (HSAC) CyberSkills Task Force Report** | • Identified 10 mission-critical cybersecurity skills.<br>• Provided recommendations to recruit, retain, and develop cybersecurity talent. | November 2012 |
| **CIO Council 2012 Information Technology Workforce Assessment for Cybersecurity** | • Provided a snapshot of the current Federal civilian IT workforce with cybersecurity responsibilities. | March 2013 |
| **National Initiative for Cybersecurity Education (NICE) National Cybersecurity Workforce Framework** | • Identified 7 categories of cybersecurity work with 31 specialty areas. Each specialty area includes a list of competencies, tasks, and sample job titles.<br>• Required by the Federal Cybersecurity Workforce Assessment Act (See below.). | April 2013 |
| **NIST Framework for Improving Critical Infrastructure Cybersecurity** | • Required by **EO 13636** in February 2013.<br>• Provided guidance for critical infrastructure organizations to better manage and reduce cybersecurity risk. | February 2014 |
| **Department of Labor (DOL) Cybersecurity Industry Competency Model** | • Provided additional competencies to include all individuals whose duties affect cybersecurity. | 2014 |
| **DOD Directive 8140.01 Cyberspace Workforce Management** | • Reissues and renumbers DOD Directive 8570. | August 2015 |

| | | |
|---|---|---|
| | • Updated and expanded established policies and assigned responsibilities for managing DOD cyberspace workforce. | |
| **Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government** | • Directed a series of actions to improve capabilities for identifying and detecting vulnerabilities and threats, enhanced protections of government assets and information, and further developed robust response and recovery capabilities for readiness and resilience when an incident inevitably occurs and addresses workforce needs. | October 30, 2015 |
| **The Federal Cybersecurity Workforce Assessment Act, contained in the Consolidated Appropriations Act of 2016 (Public Law 114-113)** | • Description of the Act: Directed the OPM data element coding structure to be fully aligned with the NICE National Cybersecurity Workforce Framework; required each Federal agency to assign the appropriate code to each position with information technology, cybersecurity, or other cyber-related functions; required a baseline assessment of the existing certifications of the cybersecurity workforce; and required the identification of the information technology, cybersecurity, or other cyber-related work roles of critical need across all Federal agencies. | December 18, 2015 |
| **Cybersecurity National Action Plan (CNAP)** | • Took near-term actions and put in place a long-term strategy to enhance cybersecurity awareness and protections, protect privacy, maintain public safety as well as economic and national security, and empower Americans to take better control of their digital security. | February 9, 2016 |
| **OMB Circular M-16-15 Federal Cybersecurity Workforce Strategy** | • Provided details on government-wide actions to identify, expand, recruit, develop, retain, and sustain a capable and competent workforce. | July 12, 2016 |
| **Executive Order 13800: Growing and Sustaining the Cybersecurity Workforce** | • Required agency heads to be guided by the NIST Framework for Improving Critical Infrastructure Cybersecurity, Feb. 2014.<br>• Required agency heads to assess cybersecurity workforce hiring and development needs. | May 17, 2017 |
| **NIST SP 800-181 – NICE National Cybersecurity Workforce Framework (NCWF)** | • Clarified, refined, and enhanced the Framework.<br>• Updates were derived from feedback NIST received since publication of Cybersecurity Framework Version 1.0. | August 2017 |
| **President's Management Agenda (PMA): Modernizing Government for the 21st Century** | • Set out a long-term vision for effective and modern government capabilities that work on behalf of the American people.<br>• Modernization efforts include: modernizing information technology, data accountability and transparency, and developing a workforce for the 21st century. | March 20, 2018 |

| | | |
|---|---|---|
| **NIST Framework for Improving Critical Infrastructure Cybersecurity Version 1.1** | • Refined, clarified, and enhanced Version 1.0, which was issued in February 2014. | April 16, 2018 |
| **Executive Order Enhancing the Effectiveness of Agency Chief Information Officers** | • Required OPM to provide CIOs delegated hiring authority for direct hire of IT positions should there exist a critical hiring need or severe shortage of candidates. | May 15, 2018 |

**NOTE:** Select the directive or model to view the content of the source.

# Definition of Cybersecurity

A critical part of identifying the cybersecurity workforce was establishing the definition of cybersecurity for consistent use throughout the Federal Government. The NICE National Cybersecurity Workforce Framework defines cybersecurity work as:

> Strategy, policy, and standards regarding the security of and operations in cyberspace, and encompass[ing] the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure.

(**Source**, Adapted from: White House Cyberspace Policy Review, May 2009)

## OPM's Cybersecurity Competency Model

In 2008, OPM partnered with the CHCO Council to prioritize occupations and job functions for future governmentwide competency models. Cybersecurity was identified as one of the occupations for which OPM was tasked with developing a competency model. Cybersecurity was selected due to:

- the impact of changes in technology, systems, and responsibilities; and
- the new and increasing demands on the cybersecurity workforce,

thus highlighting the importance of this initiative to identify key competencies of the cybersecurity workforce. The definition of cybersecurity was used as the framework in the development of OPM's competency model.

In addition to defining cybersecurity, it is important to identify key terminology related to cybersecurity work. It has been noted in numerous documents that the terms cybersecurity, computer security, information security, and information assurance should not be used interchangeably. They differ in areas of concentration (i.e., enterprise-wide, systems, and computers), methodologies, and approaches. These terms are defined below from the **NIST Glossary of Key Information Security Terms NISTIR 7298 Revision 2 – May 2013**.

- **Computer Security –** Measures and controls that ensure confidentiality, integrity, and availability of information system assets including hardware, software, firmware, and information being processed, stored, and communicated.
- **Information Security –** The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.
- **Information Assurance –** Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

The **Cybersecurity Act of 2009 (S.773)** was enacted to provide for the development of a cadre of information technology (IT) specialists to improve and maintain effective cybersecurity defenses against disruption, and for other purposes.

In November 2009, OPM initiated a **Governmentwide Cybersecurity Competency Study** to identify critical competencies for cybersecurity work, working with the CIO Council and NICE. Subject matter experts provided key insights, and employees and supervisors across the Government completed surveys to paint a comprehensive picture of cybersecurity work in the Federal Government.

Based on our collaboration with the National Security Council Interagency Policy Committee Working Group on cybersecurity education and workforce issues, the competency model was developed using the following categories:

- **IT Infrastructure, Operations, Maintenance, Computer Network Defense, and Information Assurance:** Personnel who have significant responsibilities for designing, developing, operating, or maintaining the security of Federal IT infrastructures, systems, applications and networks. Also includes individuals who have responsibility for maintaining the confidentiality, integrity, and availability of the information contained in and transmitted from those systems and networks.
- **Domestic Law Enforcement and Counterintelligence:** Personnel who analyze cyber events and environments to investigate potential threats and individuals who participate in law enforcement, counterintelligence, and other types of investigatory activities involving IT systems, networks, and/or digital information/evidence.

# Cybersecurity Characteristics

## Who performs Cybersecurity work?

One of the first challenges OPM encountered conducting this competency study was determining who performs cybersecurity work. At the time cybersecurity was an emerging field of work. As with any emerging field of work, efforts must be taken to categorize the work and identify the work requirements.

Based on our research, we were able to identify unique characteristics of cybersecurity work. The results of the OPM Competency Model Study focused on a select group of employees in various occupations responsible for cybersecurity work. The 28 occupational series covered by the survey were determined by conducting a comprehensive review of the literature and agency information we received on those who perform cybersecurity work and their supervisors. Based on participants' responses, sufficient data was collected to develop cybersecurity competency models for four occupational series – the Information Technology Management (2210), Electronics Engineering (0855), Computer Engineering (0854), and Telecommunications (0391) series. Although a fifth occupational series, Computer Scientists (1550), was identified in this study, at the time there was not sufficient information to develop a model for this series. It is noted that the four occupational series covered are the same as those mentioned in the CIO ***Net Generations: Preparing for change in the federal information technology workforce report (2010)***.

## Profiles of Cybersecurity Work

OPM developed sample task and competency profiles for the four occupational series identified in this study. The sample competency profiles in Appendix A highlight the general and technical competencies associated with each of the four occupational series – the Information Technology Management (2210), Electronics Engineering (0855), Computer Engineering (0854), and Telecommunications (0391) series. These competencies may be used in such agency efforts as workforce planning, training and development, performance management, recruitment, and selection. When used for selection, the competencies must be used in conjunction with the appropriate **OPM Qualification Standards**.

**See Appendix A for the Profiles of Cybersecurity Work.**

## Cybersecurity Competencies

OPM created a Governmentwide competency model for cybersecurity work. The competency model includes competencies by occupational series and grade levels as provided in the table below. Agencies may use these competencies to recruit and select applicants. Agencies are responsible for conducting job analyses for non-cybersecurity duties and responsibilities. Similarly, agencies must determine the applicability of these competencies to positions which do not perform the full range of cybersecurity work. Please refer to OPM's **Delegated Examining Operations Handbook** for more information on conducting a job analysis as well as OPM's **Assessment and Selection** website and select the link Job Analysis.

**Occupations and Grades with Confirmed Competencies**

| Occupations | Grades |
|---|---|
| 2210 Information Technology Management Series | 9, 11, 12, 13, 14, 15 |
| 0855 Electronics Engineering Series | 12, 13, 14, 15 |
| 0854 Computer Engineering Series | 12, 13, 14, 15 |
| 0391 Telecommunications Series | 9, 11, 12, 13 |

All positions with cybersecurity responsibilities apply common knowledge, skills, and abilities (KSAs) or competencies, organized into two areas:

- General KSAs/competencies; and
- Technical KSAs/competencies.

**See Appendix B for KSAs/competencies and definitions for all four occupations.**

## The National Cybersecurity Workforce Framework

OPM and DHS during the early stages of its collaborative endeavors co-led efforts to identify the cybersecurity workforce. With the direct engagement of over 20 Federal departments and agencies, and numerous public and private organizations, the National Initiative for Cybersecurity Education (NICE) developed the **National Cybersecurity Workforce Framework** (the Framework) to define cybersecurity work and lay a foundation for cybersecurity workforce efforts. The NICE Framework provides a common language and taxonomy, defines specialty areas and KSAs/competencies, and codifies talent.

- ***The Framework is a dictionary.*** Defining the cybersecurity population consistently and using standardized terms is an essential step in ensuring that our country is able to educate, recruit, train, develop, and retain a highly qualified workforce. The Framework lists and defines 33 specialty areas and 52 roles of cybersecurity work and provides a description of each. Each of the types of work is placed into 1 of 7 overall categories. The Framework also identifies common tasks and KSAs associated with each specialty area.
- ***The Framework is a tool.*** It provides the groundwork, or a baseline, by which organizations can develop their Human Capital Management programs, including defining roles, designing competency models, standardizing job descriptions, and providing specialized training. The Framework is used as guidance to the Federal Government, and is available to the private, public, and academic sectors for describing cybersecurity work and workforces, and related education, training, and professional development.
- ***The Framework is a collaboration.*** The Framework was developed as a direct result of the White House's conclusion that the country needed to quickly identify, quantify, and develop an effective cybersecurity workforce to develop our Nation's critical cyber infrastructure. The Framework is the output of a collaboration of over 20 Federal Departments and agencies and numerous national organizations from within academia and general industry. Each recognized a need to define the Nation's cybersecurity workforce. After an extensive review process, the first version of the Framework was finalized and approved by OMB in September 2012.

The **Framework** was updated in August 2017 to reflect changes in the workforce.

## Cybersecurity Roles/Responsibilities

In addition to categories and specialty areas, the **National Cybersecurity Workforce Framework** identifies the different roles of the cybersecurity workforce based on the duties and

responsibilities of the position. Cybersecurity work involves numerous occupations that include different disciplines. Because cybersecurity work crosses multiple occupational series, the role/work of cybersecurity differs across positions. These roles, for example, are driven by agency's mission as it relates to cybersecurity and thus influence what constitutes sound position management of agency's cybersecurity workforce.

Core roles have been identified by critical stakeholder groups in cybersecurity Governmentwide. Each of these roles includes defined tasks. Some of these roles are similar to titling guidance provided in OPM Position Classification Standards or unofficial titles agencies may uses. The two different models are provided below:

(1) NICE Framework Roles; and
(2) Roles related to U.S. Critical Infrastructure.

## (1) NICE Framework Roles

| Category | Specialty Area | Work Role | Work Role Definition |
|---|---|---|---|
| Securely Provision (SP) | Risk Management (RSK) | Authorizing Official/Designating Representative | Senior official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation (CNSSI 4009). |
| | | Security Control Assessor | Conducts independent comprehensive assessments of the management, operational, and technical security controls and control enhancements employed within or inherited by an information technology (IT) system to determine the overall effectiveness of the controls (as defined in NIST SP 800-37). |
| | Software Development (DEV) | Software Developer | Develops, creates, maintains, and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs. |
| | | Secure Software Assessor | Analyzes the security of new or existing computer applications, software, or specialized utility |

| | | | |
|---|---|---|---|
| | | | programs and provides actionable results. |
| | Systems Architecture (ARC) | Enterprise Architect | Develops and maintains business, systems, and information processes to support enterprise mission needs; develops information technology (IT) rules and requirements that describe baseline and target architectures. |
| | | Security Architect | Ensures that the stakeholder security requirements necessary to protect the organization's mission and business processes are adequately addressed in all aspects of enterprise architecture including reference models, segment and solution architectures, and the resulting systems supporting those missions and business processes. |
| | Technology R&D (TRD) | Research & Development Specialist | Conducts software and systems engineering and software systems research to develop new capabilities, ensuring cybersecurity is fully integrated. Conducts comprehensive technology research to evaluate potential vulnerabilities in cyberspace systems. |
| | Systems Requirements Planning (SRP) | Systems Requirements Planner | Consults with customers to evaluate functional requirements and translate functional requirements into technical solutions. |
| | Test and Evaluation (TST) | System Testing and Evaluation Specialist | Plans, prepares, and executes tests of systems to evaluate results against specifications and requirements as well as analyze/report test results. |
| | Systems Development (SYS) | Information Systems Security Developer | Designs, develops, tests, and evaluates information system security throughout the systems development life cycle. |
| | | Systems Developer | Designs, develops, tests, and evaluates information systems throughout the systems development life cycle. |

| | | | |
|---|---|---|---|
| Operate and Maintain (OM) | Data Administration (DTA) | Database Administrator | Administers databases and/or data management systems that allow for the secure storage, query, protection, and utilization of data. |
| | | Data Analyst | Examines data from multiple disparate sources with the goal of providing security and privacy insight. Designs and implements custom algorithms, workflow processes, and layouts for complex, enterprise-scale data sets used for modeling, data mining, and research purposes. |
| | Knowledge Management (KMG) | Knowledge Manager | Responsible for the management and administration of processes and tools that enable the organization to identify, document, and access intellectual capital and information content. |
| | Customer Service and Technical Support (STS) | Technical Support Specialist | Provides technical support to customers who need assistance utilizing client-level hardware and software in accordance with established or approved organizational process components (i.e., Master Incident Management Plan, when applicable). |
| | Network Services (NET) | Network Operations Specialist | Plans, implements, and operates network services/systems, to include hardware and virtual environments. |
| | Systems Administration (ADM) | System Administrator | Responsible for setting up and maintaining a system or specific components of a system (e.g. for example, installing, configuring, and updating hardware and software; establishing and managing user accounts; overseeing or conducting backup and recovery tasks; implementing operational and technical security controls; and adhering to organizational security policies and procedures). |
| | Systems Analysis (ANA) | Systems Security Analyst | Responsible for the analysis and development of the integration, testing, operations, and maintenance of systems security. |

| | | | |
|---|---|---|---|
| Oversee and Govern (OV) | Legal Advice and Advocacy (LGA) | Cyber Legal Advisor | Provides legal advice and recommendations on relevant topics related to cyber law. |
| | | Privacy Officer/Privacy Compliance Manager | Develops and oversees privacy compliance program and privacy program staff, supporting privacy compliance, governance/policy, and incident response needs of privacy and security executives and their teams. |
| | Training, Education, and Awareness (TEA) | Cyber Instructional Curriculum Developer | Develops, plans, coordinates, and evaluates cyber training/education courses, methods, and techniques based on instructional needs. |
| | | Cyber Instructor | Develops and conducts training or education of personnel within cyber domain. |
| | Cybersecurity Management (MGT) | Information Systems Security Manager | Responsible for the cybersecurity of a program, organization, system, or enclave. |
| | | Communications Security (COMSEC) Manager | Individual who manages the Communications Security (COMSEC) resources of an organization (CNSSI 4009) or key custodian for a Crypto Key Management System (CKMS). |
| | Strategic Planning and Policy (SPP) | Cyber Workforce Developer and Manager | Develops cyberspace workforce plans, strategies, and guidance to support cyberspace workforce manpower, personnel, training and education requirements and to address changes to cyberspace policy, doctrine, materiel, force structure, and education and training requirements. |
| | | Cyber Policy and Strategy Planner | Develops and maintains cybersecurity plans, strategy, and policy to support and align with organizational cybersecurity initiatives and regulatory compliance. |
| | Executive Cyber Leadership (EXL) | Executive Cyber Leadership | Executes decision-making authorities and establishes vision and direction for an organization's cyber and cyber-related resources and/or operations. |

| | | | |
|---|---|---|---|
| | Program/Project Management (PMA) and Acquisition | Program Manager | Leads, coordinates, communicates, integrates, and is accountable for the overall success of the program, ensuring alignment with agency or enterprise priorities. |
| | | IT Project Manager | Directly manages information technology projects. |
| | | Product Support Manager | Manages the package of support functions required to field and maintain the readiness and operational capability of systems and components. |
| | | IT Investment/Portfolio Manager | Manages a portfolio of IT investments that align with the overall needs of mission and enterprise priorities. |
| | | IT Program Auditor | Conducts evaluations of an IT program or its individual components to determine compliance with published standards. |
| Protect and Defend (PR) | Cybersecurity Defense Analysis (CDA) | Cyber Defense Analyst | Uses data collected from a variety of cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs) to analyze events that occur within their environments for the purposes of mitigating threats. |
| | Cybersecurity Defense Infrastructure Support (INF) | Cyber Defense Infrastructure Support Specialist | Tests, implements, deploys, maintains, and administers the infrastructure hardware and software. |
| | Incident Response (CIR) | Cyber Defense Incident Responder | Investigates, analyzes, and responds to cyber incidents within the network environment or enclave. |
| | Vulnerability Assessment and Management (VAM) | Vulnerability Assessment Analyst | Performs assessments of systems and networks within the network environment or enclave and identifies where those systems/networks deviate from acceptable configurations, enclave policy, or local policy. Measures effectiveness of defense-in-depth architecture against known vulnerabilities. |

| | | | |
|---|---|---|---|
| Analyze (AN) | Threat Analysis (TWA) | Threat/Warning Analyst | Develops cyber indicators to maintain awareness of the status of the highly dynamic operating environment. Collects, processes, analyzes, and disseminates cyber threat/warning assessments. |
| | Exploitation Analysis (EXP) | Exploitation Analyst | Collaborates to identify access and collection gaps that can be satisfied through cyber collection and/or preparation activities. Leverages all authorized resources and analytic techniques to penetrate targeted networks. |
| | All-Source Analysis (ASA) | All-Source Analyst | Analyzes data/information from one or multiple sources to conduct preparation of the environment, respond to requests for information, and submit intelligence collection and production requirements in support of planning and operations. |
| | | Mission Assessment Specialist | Develops assessment plans and measures of performance/effectiveness. Conducts strategic and operational effectiveness assessments as required for cyber events. Determines whether systems performed as expected and provides input to the determination of operational effectiveness. |
| | Targets (TGT) | Target Developer | Performs target system analysis, builds and/or maintains electronic target folders to include inputs from environment preparation, and/or internal or external intelligence sources. Coordinates with partner target activities and intelligence organizations, and presents candidate targets for vetting and validation. |
| | | Target Network Analyst | Conducts advanced analysis of collection and open-source data to ensure target continuity; to profile targets and their activities; and develop techniques to gain more target information. Determines how targets communicate, move, operate and live based on knowledge of |

| | | | |
|---|---|---|---|
| | | | target technologies, digital networks, and the applications on them. |
| | Language Analysis (LNG) | Multi-Disciplined Language Analyst | Applies language and culture expertise with target/threat and technical knowledge to process, analyze, and/or disseminate intelligence information derived from language, voice and/or graphic material. Creates and maintains language-specific databases and working aids to support cyber action execution and ensure critical knowledge sharing. Provides subject matter expertise in foreign language-intensive or interdisciplinary projects. |
| Collect and Operate (CO) | Collection Operations (CLO) | All Source-Collection Manager | Identifies collection authorities and environment; incorporates priority information requirements into collection management; develops concepts to meet leadership's intent. Determines capabilities of available collection assets, identifies new collection capabilities; and constructs and disseminates collection plans. Monitors execution of tasked collection to ensure effective execution of the collection plan. |
| | | All Source-Collection Requirements Manager | Evaluates collection operations and develops effects-based collection requirements strategies using available sources and methods to improve collection. Develops, processes, validates, and coordinates submission of collection requirements. Evaluates performance of collection assets and collection operations. |
| | Cyber Operational Planning (OPL) | Cyber Intel Planner | Develops detailed intelligence plans to satisfy cyber operations requirements. Collaborates with cyber operations planners to |

| | | | |
|---|---|---|---|
| | | | identify, validate, and levy requirements for collection and analysis. Participates in targeting selection, validation, synchronization, and execution of cyber actions. Synchronizes intelligence activities to support organization objectives in cyberspace. |
| | | Cyber Ops Planner | Develops detailed plans for the conduct or support of the applicable range of cyber operations through collaboration with other planners, operators and/or analysts. Participates in targeting selection, validation, synchronization, and enables integration during the execution of cyber actions. |
| | | Partner Integration Planner | Works to advance cooperation across organizational or national borders between cyber operations partners. Aids the integration of partner cyber teams by providing guidance, resources, and collaboration to develop best practices and facilitate organizational support for achieving objectives in integrated cyber actions. |
| | Cyber Operations (OPS) | Cyber Operator | Conducts collection, processing, and/or geolocation of systems to exploit, locate, and/or track targets of interest. Performs network navigation, tactical forensic analysis, and, when directed, executes on-net operations. |
| Investigate (IN) | Cyber Investigation (INV) | Cyber Crime Investigator | Identifies, collects, examines, and preserves evidence using controlled and documented analytical and investigative techniques. |
| | Digital Forensics (FOR) | Law Enforcement /CounterIntelligence Forensics Analyst | Conducts detailed investigations on computer-based crimes establishing documentary or physical evidence, to include digital media and logs associated with cyber intrusion incidents. |

| | | | |
|---|---|---|---|
| | | Cyber Defense Forensics Analyst | Analyzes digital evidence and investigates computer security incidents to derive useful information in support of system/network vulnerability mitigation. |

Source: **NIST Special Publication 800-181 National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework, 2017**

### (2) Critical Infrastructure Roles

New cyber roles were developed to support a Federal agency's mission and responsibilities to protect United States infrastructure. The President issued a Presidential Policy Directive, **PPD-21**, Critical Infrastructure (CI) Security and Resilience directive, which identifies 16 critical infrastructure sectors and designates associated Federal Sector-Specific Agencies (FSSAs). In some cases co-FSSAs are designated where those departments share the roles and responsibilities of the FSSA.

The CI sectors and FSSAs are as follows:

| **Critical Infrastructure Sectors** | **Federal Sector-Specific Agencies** |
|---|---|
| Chemical | Department of Homeland Security |
| Commercial Facilities | Department of Homeland Security |
| Communications | Department of Homeland Security |
| Critical Manufacturing | Department of Homeland Security |
| Dams | Department of Homeland Security |
| Defense Industrial Base | Department of Defense |
| Emergency Services | Department of Homeland Security |
| Energy | Department of Energy |
| Financial Services | Department of the Treasury |
| Food and Agriculture | U.S. Department of Agriculture and Department of Health and Human Services |
| Government Facilities | Department of Homeland Security and General Services Administration |
| Healthcare and Public Health | Department of Health and Human Services |
| Information Technology | Department of Homeland Security |
| Nuclear Reactors, Materials, and Waste | Department of Homeland Security |
| Transportation Systems | Department of Homeland Security and Department of Transportation |
| Water and Wastewater Systems | Environmental Protection Agency |

Sources: **NICE Cybersecurity Workforce Framework, 2017**; **Cybersecurity Workforce Framework Interactive How-To and Implementation Guide**, 2012

## OPM Cybersecurity Category/Specialty Area Code

In addition to our collaboration with the NICE effort and work with other stakeholders, there was a need to identify the cybersecurity workforce Governmentwide using another approach. To do so, OPM embarked on an effort to identify cybersecurity positions Governmentwide and developed the Cybersecurity Category/Specialty Area Code. The Cybersecurity Category/Specialty Area code is used to identify incumbents or positions for which the primary work is cybersecurity. Cybersecurity is an evolving area and positions may be classified in a number of different occupational series based on the nature of the work. Use of this code will enable OPM and Federal agencies to more effectively identify the cybersecurity workforce, determine baseline capabilities, examine hiring trends, identify skill gaps, and more effectively recruit, hire, train, develop, and retain an effective cybersecurity workforce.

Agencies must use the **Federal Cybersecurity Coding Structure** to find the Cybersecurity Data Standard Codes to assign to encumbered and vacant positions. The codes represent the various work roles found in information technology, cybersecurity, and cyber-related functions. The Cybersecurity Data Standard Codes in the Federal Cybersecurity Coding Structure are also described in **OPM's Guide to Data Standards**. Agencies may code up to three substantial functions per position; therefore, they should assign the Cybersecurity Data Standard Codes in the order in which the most critical function of the job is listed first, the next critical function of the job is listed next, and so on.

Please refer to the **Federal Cybersecurity Workforce Assessment Act MAX page** for periodic updates and helpful resources for applying the revised Cybersecurity Data Standard Codes and carrying out other requirements of the Act.

# CYBERSECURITY CLASSIFICATION POLICY GUIDANCE

## Cybersecurity Classification

Federal Agencies have identified developing effective human resources (HR) practices for the Federal Cybersecurity Workforce as mission-critical, and are working to recognize and close competency gaps in these areas. OPM is providing the following guidance for classifying cybersecurity work in the Federal Government.

Based on OPM's collaboration with our agency partners and critical work with stakeholders, the data and information collected identify that the majority of cybersecurity work in the Federal government is classified to the **Job Family Standard (JFS) for Administrative Work in the Information Technology Group, 2200**.

**The following policy is effective immediately upon issuance of this guidance:**

1. **OPM has prescribed an official/basic title, IT Cybersecurity Specialist, to the IT 2210 Management Series for immediate titling of positions in the 2210 series that include cybersecurity work. This title may be used in conjunction with/without the 11 parenthetical titles in the IT Management Series, 2210 (See section Parenthetical Titles). Positions classified to the IT Management Series, 2210 must require IT knowledge and IT competencies. Furthermore, this work must be coded to include cybersecurity functions as supported by the job codes in the Guide to Data Standards and the NICE Cybersecurity Workforce Framework, 2017.**

2. **Other occupational series performing cybersecurity work may use Cybersecurity as a parenthetical title if cyber work is performed the majority of the time, and not as a collateral duty, and as supported by the job codes in the Guide to Data Standards and the NICE Cybersecurity Workforce Framework, 2017 (See section Parenthetical Titles).**

# Classifying Positions with Cybersecurity Work

When classifying a position, the following must be determined:

- The proper pay system;
- The proper occupational series;
- The official position title; and
- The proper grade or level of work.

## Determining the Pay System

Positions with cybersecurity responsibilities usually are General Schedule (GS) positions. However, some positions may be Senior Executive Service (SES) positions or Senior Level (SL) or Scientific/Professional (ST) positions. Guidance for identifying such positions above the GS-15 grade level can be found later in this section. This guidance is not intended for Federal Wage System (FWS) positions.

Note: The classification of a position is used to determine certain pay entitlements of an employee in that position. Agencies should remain aware that changes in the pay system, occupational series, title, or grade level of a position could affect how an employee in that position will be paid. For example, coverage under special rates established under 5 U.S.C. 5305 and 5 CFR part 530, subpart C, is dependent on the position's pay system, occupational series, grade level, and, at times, official title.

## Determining Occupational Series of Positions with Cybersecurity Work

The cybersecurity workforce is occupationally cross-cutting, multi-faceted, and encompasses a variety of contexts, roles, and occupations. It requires a cadre of different backgrounds and experience to perform the cybersecurity work required by agencies. Cybersecurity work performed by IT Specialists in the 2210 Series must be determined by proper application of the 2200 IT Management JFS. When cybersecurity work is included in other established occupations and covered by more than one occupational series, a classification determination can be made by reviewing the duties and responsibilities assigned to the position. In most instances, the primary work of the position, the highest level of work performed, and the paramount occupational knowledge for the work dictate the appropriate series.

Users of the position classification standards normally have little trouble making the series decision by comparing the characteristics of the position in question to series definitions and occupational information in the standards. However, if the work of a position falls into more than one series, the correct series is sometimes difficult to determine. If it is unclear whether a particular series predominates, consider the following to determine the appropriate series:

- ***Paramount occupational knowledge required.*** Some positions may include several different kinds of work; however, most positions have a paramount occupational knowledge requirement in addition to the cybersecurity knowledge, skills, and abilities/competencies. The paramount occupational knowledge is the most important subject matter knowledge or subject-related experience required to do the work.
- ***Reason for existence.*** The primary purpose for the existence of the position, or management's intent in establishing the position, is a positive indicator in determining the appropriate series.
- ***Organizational mission and/or function.*** Since cybersecurity is critical work within an organization, it may generally be aligned with the mission and function of the organization to which they are assigned. The organization's function often is mirrored in the organizational title and may influence the choice of appropriate series.
- ***Recruitment source.*** Supervisors and managers can help by identifying the occupational series that provides the best qualified applicants to do the work. This aspect correlates with the paramount knowledge required by the position.

Cybersecurity work can be characterized as multidisciplinary. A multidisciplinary position is a position involving duties and responsibilities closely related to more than one discipline. As a result, the position could be classifiable to two or more occupational series. The nature of the work is such that persons with training and experience in either of two or more occupations may be considered well-qualified to do the work.

NOTE**:** Due to the evolution of work in cybersecurity, the term multidisciplinary is used to more appropriately define the unique and occupationally cross-cutting combinations of work in this discipline. While this term is not addressed in the current Introduction to the Position Classification Standards or the Classifier's Handbook, future updates will address the usage of this terminology.

Multidisciplinary positions generally fall into one of the following two categories:

- Positions which involve a specific *combinatio*n of knowledges that is characteristic of two or more non-professional series. Such positions involve the performance of some duties which are characteristic of one series and other duties which are characteristic of another series.

- Positions which involve knowledge which is characteristic of *either* two or more non-professional series. These positions include work which is substantially identical to work performed in either of the non-professional occupations.

The position description should show clearly that the position is multidisciplinary and indicate the various series in which the position may be classified. The final classification of the position is determined by the qualifications of the person selected to fill it.

Positions are not to be considered multidisciplinary when members of a work team with varied but complimentary competencies and experiences collaborate on a multifaceted problem or project and contribute to the achievement of organizational specific objectives. Also excluded are positions which require special licensing, as in the practice of medicine, and positions which are solely and clearly classifiable to a single series but can be filled by persons from a variety of education and experience backgrounds. Work requiring professional backgrounds including education and experience are considered interdisciplinary. Professional occupations may not be combined with non-professional occupations or viewed as interdisciplinary positions. For further guidance on interdisciplinary positions reference the discussion on Interdisciplinary Professional Positions in Section III L. in the **Introduction to the Position Classification Standards**.

## Determining Official Position Titles

The law (5 U.S.C. 5105 (a)(2)) requires OPM to establish the official titles of positions in published classification standards. Accordingly, position classification standards generally prescribe the titles to be used for positions in the covered series. Only the prescribed title may be used on official documents relating to a position (e.g., position descriptions and personnel actions).

The requirement to use official titles (5 U.S.C. 5105(c)), however, does not preclude agencies from using any unofficial title they choose for positions. Agencies may use organizational or other titles for internal administration, public convenience, or similar purposes.

In those instances where OPM has not prescribed an official title for a series, an agency may designate an official title. According to the **Introduction to the Position Classification Standards**, constructed titles should be "short," "meaningful," and "generally descriptive of the work performed." All titling should be used consistently throughout the agency.

**IT Cybersecurity Specialist Official/Basic Position Title**

**OPM Memorandum, Official Position Title for Cybersecurity Positions, dated October 2018, amends the Job Family Standard for Administrative Work in the Information Technology Group, 2200, dated October 2018, and authorizes IT Cybersecurity Specialist as an official/basic title for this function when it is characterized by the common set of duties/tasks described on page 15 - "Cybersecurity Classification". This guidance also authorizes the use of cybersecurity as a parenthetical title for other occupational series performing cyber functions the majority of the time as described on page 15 – "Cybersecurity Classification".**

### Titling Guidance for 2210 IT Occupational Series Positions

The IT 2210 Series as amended includes the basic or official title, IT Cybersecurity Specialist. Agencies may use the 11 parenthetical titles in the IT 2210 Series in conjunction with the basic/official title, IT Cybersecurity Specialist. The parenthetical titles may supplement an official or basic title and should only be used when the position requires work characterized by the parenthetical title. In application a 2210 position may include the following basic title and parenthetical title: IT Cybersecurity Specialist (INFOSEC) and IT Cybersecurity Manager (PLCYPLN).

### Titling Guidance for other Occupational Series including Cybersecurity Duties

Agencies with positions including cybersecurity work as outlined in this guidance may supplement the basic position titles by adding parenthetical titles, where necessary, to identify cyber duties and responsibilities which reflect specific cyber knowledge and skills required in the work. Parenthetical titles may be necessary for recruitment purposes and meeting other organizational needs.

Agencies may also supplement the basic/official position titles by adding the parenthetical title, cybersecurity, to other occupational series including cybersecurity functions, not classified to the 2210 IT Series. The requirements as prescribed on page 15 - "Cybersecurity Classification" must be met. For example, other series performing cyber work may be titled Computer Engineer (CYBER) or Computer Scientists (CYBER).

### Official Specialty or Parenthetical Titles

In addition to this titling guidance agencies may also use specialty titles. Specialty titles are typically displayed in parentheses and referred to as parenthetical titles as well. Parenthetical titles, as defined above, may be used with the basic/official title of the position to further identify the duties and responsibilities performed and the special knowledge and skills needed. As an example the 31 Specialty Areas as defined in the **National Cybersecurity Workforce**

**Framework** may be used as a specialty parenthetical title, IT Cybersecurity Specialist (Incident Responder/Digital Forensics).

Agencies should use the basic/official title without a parenthetical specialty title for positions with no established specialty or emphasis area or for positions involving work in more than two of the established specialties.

Agencies may also combine two authorized parenthetical specialty titles (e.g., Applications Software/Systems Analysis) when the two specialties are significant to the position. You may continue to use other agency-established parenthetical titles where appropriate as unofficial position titles; i.e., organizational or functional titles.

### Organizational Titles

Organizational and functional titles do not replace, but complement, official position titles. Agencies may establish organizational and functional titles for internal administration, public convenience, or similar purposes. Examples of organizational titles are Cybersecurity Branch Chief and Cybersecurity Division Chief. Examples of functional titles are Cybersecurity Analyst, Chief Information Cybersecurity Officer and Director of Cybersecurity.

## Applying Grading Criteria to Positions with Cybersecurity Work

According to the **Introduction to the Position Classification Standards**, selecting the appropriate grade level criteria is critical for determining the proper classification of a position. If the work assigned to a position is adequately covered by the grading criteria in a particular standard for a specific occupational series or job family, then evaluate the work by that occupational series or job family standard (JFS). This includes positions with cybersecurity responsibilities.

If the type of work does not have a directly applicable occupational series, job family, or functional standard, then select a standard as similar as possible to the kind of work described. Evaluate and grade the work in question by comparing it to grading criteria in the comparable standard, as it relates to:

- The kind of work processes, functions, or subject matter of the work performed;
- The qualifications required to do the work;
- The level of difficulty and responsibility necessary; and
- The combination of classification factors having the greatest influence on the grade level.

When making these determinations, we recommend referring to one of the following standards for making meaningful comparisons:

- The **JFS for Administrative Work in the Information Technology Group, 2200**, to evaluate positions in the IT occupation with cybersecurity responsibilities;
- The **JFS for Professional and Administrative Work in the Accounting and Budget Group, GS-0500**, or the **Financial Management Series, GS-0505**, to evaluate cybersecurity role for financial systems;

- The **JFS for Administrative Work in the Inspection, Investigation, Enforcement, and Compliance Group, GS-1800,** to evaluate investigation positions with cybersecurity role;
- The **Administrative Analysis Grade Evaluation Guide** to evaluate positions with cybersecurity where a more closely related standard has not been issued;
- Part II of the **Equipment Development Grade Evaluation Guide** to evaluate positions when cybersecurity collaborates with engineers;
- The **Professional Work in the Engineering and Architecture Group, 0800**, to evaluate positions with cybersecurity roles;
- The **Position Classification Flysheet for Computer Science Series, GS-1550**, to evaluate positions with cybersecurity roles;
- The Position Classification Standard for Telecommunications Series, GS-0391, to evaluate such positions with cybersecurity roles;
- The Position Classification Flysheet for Government Information Series, 0306, to evaluate positions with cybersecurity roles in establishing, safeguarding, disseminating or managing Government information;
- The **Position Classification Flysheet for Records and Information Management Series, 0308**, to evaluate positions with cybersecurity roles; and
- The **Position Classification Standard Flysheet for Intelligence Series, GS-0132**, to evaluate positions with cybersecurity roles.

**Note:** If a position with cybersecurity work exercises supervision of Federal Government employees at a level that meets the criteria indicated in **General Schedule Supervisory Guide**, be sure to evaluate the position's supervisory duties. Do not classify such position to a lower grade on the basis of personal work accomplishment rather than the proper grade for supervising staff of the type and level actually involved.

## Applying Grading Criteria to IT Positions with Cybersecurity Functions

Since the majority of individuals with cybersecurity responsibility are found in the 2210 series, we are using that occupation as an example. Criteria for grading positions with cybersecurity work in the Information Technology Management Series, GS-2210 are found in the **JFS for Administrative Work in the Information Technology Group, 2200**. The grade level of an IT position with cybersecurity work, GS-2210 position will depend on the nature of the work as constrained by the relationship of its scope, resources, and timeline (e.g., its size, risk, sensitivity). Selecting appropriate grade level criteria is a primary decision in determining the proper classification of work. The criteria selected as the basis for comparison should be for a kind of work as similar as possible to that of the position being evaluated.

**Cybersecurity** work is defined in the Information Technology Management Series, GS-2210 in the JFS for Administrative Work in the Information Technology Group, 2200.

The example on the following page illustrates how Factor 1 (Knowledge Required by the Position) applies to the duties of a particular IT Cybersecurity Specialist, GS-2210-12 or GS-2210-13 position. The factor level descriptions (FLDs) are based on the cybersecurity work performed at Federal agencies as classified by the JFS for Administrative Work in the Information Technology Group, 2200.

# Example: IT Cybersecurity Specialist, 2210

**FLD 1-7: IT Cybersecurity Specialist, 2210 (Illustration #1)**

Knowledge of and skill in applying:

- methods used to evaluate implement, and disseminate IT security tools and procedures;
- IT security certification and accreditation requirements;
- network operations and protocols; or computer forensics principles.

sufficient to:

- develop, implement, and coordinate activities designed to ensure, protect, and restore IT systems, services and capabilities;
- monitor and evaluate systems' compliance with IT security requirements;
- provide advice and guidance on implementing IT security policies and procedures in the development and operation of network systems; and /or
- ensure proper protection of evidence used in investigating computer crimes.

**FLD 1-8: IT Cybersecurity Specialist (Incident Responder/Digital Forensics), 2210 (Illustration #2)**

Mastery of and skill in applying:

- total infrastructure protection environments;
- systems security certification and accreditation requirements and processes; and /or
- Federal information systems security protocols.

sufficient to:

- integrate information systems security with other security disciplines;
- certify systems or network accreditation; and /or
- ensure coordination and/or collaboration on security activities.

Using the IT Management 2200 JFS to evaluate the duties listed on the previous page could result in classifying the position across all nine factors in the Factor Evaluation System as an IT Cybersecurity Specialist, GS-2210-11:

| Factor | Level | Points |
|---|---|---|
| 1. Knowledge Required | 1–7 | 1,250 |
| 2. Supervisory Controls | 2–4 | 450 |
| 3. Guidelines | 3–3 | 275 |
| 4. Complexity | 4–4 | 225 |
| 5. Scope & Effect | 5–3 | 150 |
| 6 & 7. Contacts & Purpose | 3–B/C | 180 |
| 8. Physical Demands | 8–1 | 5 |
| 9. Work Environment | 9–1 | 5 |
| **Total Points** | | 2,540 |
| **Conversion** | | GS-11 |

Using the IT Management 2200 JFS to evaluate the duties listed on the previous page could result in classifying the position across all nine factors in the Factor Evaluation System as an IT Cybersecurity Specialist, GS-2210-12:

| Factor | Level | Points |
|---|---|---|
| 1. Knowledge Required | 1–7 | 1,250 |
| 2. Supervisory Controls | 2–4 | 450 |
| 3. Guidelines | 3–4 | 450 |
| 4. Complexity | 4–4/5 | 225 |
| 5. Scope & Effect | 5–4/5 | 225 |
| 6 & 7. Contacts & Purpose | 3–C | 180 |
| 8. Physical Demands | 8–1 | 5 |
| 9. Work Environment | 9–1 | 5 |
| **Total Points** | | 2,790 |
| **Conversion** | | GS-12 |

Using the IT Management 2200 JFS to evaluate duties could result in classifying the position across all nine factors in the Factor Evaluation System as an IT Cybersecurity Specialist, GS-2210-13:

| Factor | Level | Points |
|---|---|---|
| 1. Knowledge Required | 1–8 | 1,550 |
| 2. Supervisory Controls | 2–4 | 450 |
| 3. Guidelines | 3–4 | 450 |
| 4. Complexity | 4–5 | 325 |
| 5. Scope & Effect | 5–5 | 325 |
| 6 & 7. Contacts & Purpose | 3–C | 230 |
| 8. Physical Demands | 8–1 | 5 |
| 9. Work Environment | 9–1 | 5 |
| **Total Points** | | 3,340 |
| **Conversion** | | GS-13 |

**NOTE:** The above tables show examples only. They do not preclude the use of other factor levels that may be appropriate depending on the assignment of duties and responsibilities to a particular position.

## Identifying Positions above the GS-15 Grade Level

Agencies are responsible for managing their executive resources and deciding how to organize functions and structure positions, including positions with cybersecurity work, in a manner that best meets the organization's mission requirements. This includes deciding whether positions meet the Senior Executive Service (SES) criteria or the Senior Level (SL) or Scientific/Professional (ST) criteria and establishing individual SES, SL, and ST positions within the agency's executive resource allocation as authorized by OPM.

The law and OPM regulations clearly state that SES, SL, and ST positions must be classifiable **above the GS-15 grade level**. Positions at the GS-15 grade level as described in statute clearly cover a broad range of work: *Grade GS-15 includes those classes of positions the duties of which are to perform, under general administrative direction, with very wide latitude for the exercise of independent judgment, work of outstanding difficulty and responsibility along special technical, supervisory, or administrative lines which has demonstrated leadership and exceptional attainments* (5 U.S.C. 5104(15)). Do not assume a position is above the GS-15 grade level simply because it has a somewhat larger scope or requires more knowledge and skill than another position with cybersecurity work that is already classified at GS-15.

Distinctions among the SES, SL, and ST positions are not always clear. The following information provides general guidance to help agencies identify SES, SL, and ST positions; maintain an agency's flexibility to manage its executive resources; and contribute to intra- and inter-agency consistency in establishing SES, SL, and ST positions.

**General Information** - Unless an agency is excluded from the SES by statute or by the President of the United States, any position that is classifiable above the GS-15 grade level **and** which meets the functional executive criteria set forth in 5 U.S.C. 3132(a)(2) may be placed in the SES. Positions that are classifiable above the GS-15 grade level that do **not** meet the executive criteria and involve the performance of high-level research and development in the physical, biological, medical, or engineering sciences are more appropriately placed in the ST system. The SL system includes any other positions that are classifiable above the GS-15 grade level and do **not** meet the executive criteria and do **not** involve the fundamental research and development responsibilities characteristic of ST positions.

**SES Criteria** - 5 U.S.C. 3132(a)(2) sets forth the criteria that characterize SES positions. SES positions must be classifiable **above the GS-15 grade level**, or equivalent, based on the duties, responsibilities, and qualifications required by the position. In addition, the incumbent **must** engage in one of the following activities:

- Directing the work of an organizational unit;
- Being accountable for the success of one or more specific programs or projects;
- Monitoring progress toward organizational goals and periodically evaluate and make appropriate adjustments to such goals;
- Supervising the work of employees (other than personal assistants); or
- Otherwise exercising important policy-making, policy-determining, or other executive functions.

***Directing the work of an organizational unit*** to manage a program includes responsibility for:

- Assessing policy, program, and project feasibility;
- Determining program goals and developing implementation tools;
- Designing an organizational structure to promote effective work accomplishment; and
- Setting effectiveness, efficiency, productivity, and management/internal control standards.

***Being accountable for the success of a program that*** encompasses responsibility for the full range of factors that affect IT program management along with a cybersecurity role and accomplishment. This includes:

- Obtaining the resources necessary to achieve the desired program objective;
- Assuming responsibility for the effective use of government resources; and
- Dealing with key officials both within and outside the organization to gain understanding and support for all aspects of the program and program functions.

***Monitoring progress toward organizational goals and making appropriate adjustments*** is an extension of an individual's responsibility for directing the work of an organizational unit. It includes:

- Monitoring work status through formal and informal means to evaluate progress toward objectives;
- Assessing overall effectiveness, efficiency, and productivity of the organization;
- Identifying, diagnosing and consulting on problem areas related to implementation and goal achievement; and
- Making decisions regarding alternative courses of action.

***Supervising the work of employees*** should be credited only if the position meets the minimum requirements for coverage under OPM's **General Schedule Supervisory Guide**. Specifically, the position's supervisory responsibilities must:

- Require accomplishment of work through the combined technical and administrative direction of others;
- Constitute a major duty occupying at least 25 percent of the incumbent's time; and
- Meet at least the lowest level of Factor 3 in the guide based on supervision of non-contractor personnel. (Work performed by contractors is considered in applying the grading criteria within each factor of the supervisory guide, provided the position first meets the coverage requirements above based on supervision of non-contractor personnel).

***Policy-making or policy-determining functions*** include responsibility for reviewing staff recommendations on policies developed to affect the organization's mission; considering political, social, economic, technical, and administrative factors with potential impact on recommended policies; and approving those policies.

It would be unusual to find a position that entails making major policy decisions.

**Distinguishing Between SES and SL/ST Positions –** Positions that are properly classified above the grade GS-15 grade level, and do **not** meet the functional executive criteria, are more appropriately placed in the Senior Level (SL) or Scientific/Professional (ST) systems. The nature of a position's work determines which system is most appropriate.

- ***Senior Level (SL) Positions.*** SL positions are classifiable **above the GS-15 grade level**, but do **not** meet the executive criteria characteristic of the SES, nor do they involve the fundamental research and development responsibilities characteristic of ST positions. SL positions may include some supervisory and related managerial duties, provided these duties occupy less than 25 percent of the position's time.

  **NOTE**: In some instances, the SL system is used for positions that meet the SES executive criteria in agencies that have been excluded from the SES.

- ***Scientific/Professional (ST) Positions*.** ST positions are classifiable **above the GS-15 grade level** and involve the performance of high-level research and development in the physical, biological, medical, or engineering sciences (or closely related field). ST positions may include some supervisory and related managerial duties, provided these

duties occupy less than 25 percent of the position's time. Given the characteristics of project manager work, it is unlikely to occur in ST positions.

# Qualifying and Ranking Applicants

## Qualifying Applicants

***Governmentwide minimum qualification standards*** are published in OPM's **Operating Manual: Qualification Standards for General Schedule Positions**. Most qualification standards permit applicants to qualify on the basis of education/training, experience, or a combination of the two. They include the patterns of education, training, and/or experience most commonly applicable to a particular occupational series. Some qualification standards, however, have specific educational, licensure, or certification requirements that may apply only to specific positions in an occupational series. Agencies and examining offices should select the qualification standard that covers the occupational series to which a position has been classified.

Because cybersecurity work usually requires unique competencies based on agencies' mission, agencies must determine the paramount knowledge required for occupations that includes cybersecurity. After identifying the appropriate occupation, selection of the proper qualification standard can be made. The occupational knowledge determines the series of a position for classification purposes (see **Determining Occupational Series of Positions with Cybersecurity Work**, pp. 21 and 22). It also determines the qualifications standard used to screen qualifications of applicants. However, for occupations with cybersecurity work, agencies must include specific cybersecurity competencies to select an individual to fill any position with cybersecurity work. For minimum qualifications, use the qualification standard appropriate for the occupational series.

Agencies may supplement minimum qualifications with additional KSAs/competencies identified through a job analysis. A job analysis is a systematic method of studying a job to identify the tasks performed and link them to the KSAs/ competencies required to perform these tasks. Where appropriate, and supported by a job analysis, agencies may use the competency as a selective factor or quality ranking factor. For additional information on conducting a job analysis and establishing selective and quality ranking factors, agencies may consult **OPM's Delegated Examining Operations Handbook**.

***Selective factors*** become part of the minimum requirements for a position. A selective factor is a "screen out" (i.e., if an applicant does not meet a selective factor he/she is ineligible for further consideration).

Selective factors:

- Are essential for successful performance on the job (i.e., if individuals do not have the selective factor, they cannot perform the job);
- Are almost always geared toward a specific technical KSA/competency;
- Require extensive training or experience to develop; and
- Cannot be learned on the job in a reasonable amount of time.

Selective factors cannot be so narrow that they preclude from consideration applicants who could perform the duties of the position. Agencies may not use selective factors that could be learned readily during the normal period of orientation to the position. Nor should agencies use selective factors that are so agency specific that they exclude from consideration applicants without prior Federal service or preclude selection of applicants from priority placement lists established to assist in the placement of employees affected by reductions in force. Examples of KSAs/competencies that **should not** be used as selective factors include knowledge of:

- An organization's policies and planning processes; and
- An agency's rules, regulations, policies, and guidance.

**Note:** When using a selective factor, you must specify the required proficiency level.

## Ranking Qualified Applicants

***Quality ranking factors*** are KSAs/competencies that significantly enhance performance in a position, but, unlike selective factors, are not essential for satisfactory performance. Agencies should rank applicants with higher proficiency levels on a quality ranking factor above those with lower proficiency levels. Agencies may not rate qualified candidates ineligible solely for failure to possess a quality ranking factor. With quality ranking factors, the focus is on the level of proficiency the candidate brings to the job.

## Justification and Documentation

Agencies must document both selective factors and quality ranking factors through job analysis by identifying the:

- KSAs/competencies basic to and essential for satisfactory job performance;
- Duties/tasks the incumbent will perform that require possessing the required KSAs/competencies; and
- Education, experience, or other qualifications that provide evidence of the possession of the required KSAs/competencies.

## Certification

OPM has not established certification requirements for the cybersecurity workforce. However, agencies may specify a particular type of certification (or equivalency) in establishing selective criteria or in defining quality ranking factors. Subject matter experts must determine that the certification is necessary for satisfactory job performance (i.e., the certification is related to the duties/tasks and required KSAs/competencies of the job). The certification may then be used as evidence validated by a job analysis that a person has the KSAs/competencies needed to perform cybersecurity work at a satisfactory level.

# Assessment Policy and Tools

Applicable law requires the use of effective assessments in the hiring process, and OPM promotes their use for practical reasons as well. The use of effective assessments addresses barriers to recruiting and hiring the talent needed in agencies to perform the cybersecurity work of the agency and improves the quality and diversity of hires. In addition, the use of effective assessments in the hiring process provides human resources professionals and hiring managers the tools and resources needed to support their recruiting and hiring efforts and increase hiring manager satisfaction with the quality of applicants. This requires the collaboration between HR and hiring managers to develop and design effective assessment strategies to hire the talent needed to perform the cybersecurity work of your agency.

Agencies should standardize and document the assessment process through the following steps:

- Treat all individuals consistently. This is most easily accomplished by adopting a standardized assessment and decision-making process. "Standardizing" means making a process uniform to ensure the same information is collected on each individual and is used in a consistent manner in employment decisions.
- Ensure the selection tool is based on an up-to-date job analysis and is supported by strong validity evidence. A validation study can verify that applicants who score well on the selection device are more likely to do well on the job and contribute to organizational success. Agencies not familiar with validation research methodology are encouraged to consult a measurement expert.

OPM offers various assessments resources and tools for agency use. The following highlights our policy, tools and educational resources available to agencies.

## Policy

**Assessment & Selection Website** – contains resources to learn more about personnel assessment, assessment methods, steps to designing effective assessment strategies, and the importance of effective personnel assessment.

**Delegated Examining Operations Handbook (DEOH)**, contains information on the assessment process and policy.

- **Chapter 2**– Identifying the Job and its Assessments (p. 22);
- **Chapter 5** – Assess Applicants (p.90);
- **Appendix F** – Multipurpose Occupational Systems Analysis (p. 233); and
- **Appendix G** – OPM's Job Analysis Methodology (p. 275).

**Interagency Assessment Policy Forum** – Interagency work group with the focus to improve assessments Governmentwide. Contact us at **assessment_information@opm.gov**.

## Tools

**Assessment Decision Tool (ADT)** – OPM's automated system developed to help Federal agencies evaluate and improve their hiring processes and thus continuously build and sustain an

effective civilian workforce for the Federal Government. The system is designed to help human resources professionals and hiring supervisors/managers develop assessment strategies targeted to specific competencies and other situational factors relevant to their hiring situation (e.g., volume of applicants, level of available resources). The ADT is designed to provide you with customized information based on your specific hiring needs.

**USA Hire** – The USA Hire[SM] assessment battery can be used in conjunction with the traditional occupational questionnaire, and/or additional assessments, such as a Structured Interview, to target agency-specific job requirements. USA Hire[SM] offers the following advantages:

- Objective, professionally-developed assessments
- An efficient and effective tool for evaluating candidates
- Meets all legal guidelines and professional standards
- Applicant friendly
- Ease of implementation as it is already fully integrated with USA Staffing®
- Advanced technology to include computer adaptive testing
- Whole person assessments allow agencies to target critical job-relevant competencies
- More valid measures of applicant competence, reinforced by decades of research supporting the validity of USA Hire[SM] type assessment results

### Educational Resources

**OPM's Assessment and Selection** website includes presentations and tools that agencies may use to develop an assessment strategy and to learn more about various assessment tools and the use of assessments to meet agency specific needs in hiring (e.g., Assessing Students and Recent Grads).

### Other Resources

**OPM Cybersecurity Pay and Hiring Authorities** – This memorandum provides information on a number of hiring, pay, and leave flexibilities that agencies may use to fill and retain individuals in cybersecurity positions.

## Further Guidance

This guidance will help you classify and fill positions in an occupation with cybersecurity responsibilities. If you have questions about this guide, contact the appropriate OPM office as follows:

- Classification/Qualifications Policy – **FedClass@opm.gov**
- Assessment Policy – **Assessment_Information@opm.gov**
- Employment or staffing issues – **Employ@opm.gov**
- Pay and Leave Policy – **pay-leave-policy@opm.gov**
- Training and employee development topics – **HRD@opm.gov**

# Appendix A – Profiles of Cybersecurity Work

## Important Competencies and Tasks by Occupation

| 2210 Information Technology Management Series | | |
|---|---|---|
| **Important Competencies** | | |
| Accountability | Information Management | Reading |
| Attention to Detail | Information Systems Security Certification | Reasoning |
| Communications Security Management | Information Systems/Network Security | Resilience |
| Compliance | Integrity/Honesty | Security |
| Computer Network Defense | Interpersonal Skills | Self-Management |
| Computer Skills | Leadership | Stress Tolerance |
| Configuration Management | Learning | Teaching Others |
| Creative Thinking | Memory | Teamwork |
| Customer Service | Operating Systems | Technical Competence |
| Decision Making | Oral Communication | Writing |
| Flexibility | Planning and Evaluating | |
| Information Assurance | Problem Solving | |
| **Important Tasks** | | |
| Makes improvements, solves problems, or takes corrective action when problems arise. | | |
| Recommends improvements or solutions to problems, or determines appropriate actions. | | |
| Identifies or anticipates needs or problems. | | |
| Monitors own progress on work products against assigned goals. | | |
| Promotes or develops and maintains good working relationships with key individuals or groups. | | |
| Provides technical advice or assistance to others. | | |
| Develops and maintains relationships with customers with diverse needs. | | |
| Uses computer systems or applications to access, create, edit, print, send, retrieve, or manipulate data, files, or other information. | | |
| Collaborates with others or works on teams to accomplish work-related activities. | | |

| 0855 Electronic Engineering Series | | |
|---|---|---|
| **Important Competencies** | | |
| Accountability | Flexibility | Reading |
| Attention to Detail | Integrity/Honesty | Reasoning |
| Communications Security Management | Interpersonal Skills | Resilience |
| Compliance | Leadership | Self-Management |
| Computer Skills | Learning | Stress Tolerance |
| Creative Thinking | Memory | Teamwork |
| Customer Service | Oral Communication | Technical Competence |
| Decision Making | Planning and Evaluating | Writing |
| Engineering and Technology | Problem Solving | |
| **Important Tasks** | | |
| Monitors own progress on work products against assigned goals. | | |
| Makes improvements, solves problems, or takes corrective action when problems arise. | | |
| Promotes or develops and maintains good working relationships with key individuals or groups. | | |
| Recommends improvements or solutions to problems, or determines appropriate actions. | | |
| Identifies or anticipates needs or problems. | | |
| Collaborates with others or works on teams to accomplish work-related activities. | | |
| Attends briefings, meetings, conferences, or hearings. | | |
| Gives presentations or briefings. | | |
| Justifies and explains decisions, conclusions, findings, or recommendations. | | |
| Develops and maintains relationships with customers with diverse needs. | | |
| Reviews and provides feedback on the content of complex information (for example, research on contract proposals, financial, technical, or management reports). | | |
| Analyzes or interprets data or other information. | | |
| Reviews reports, documents, records, data, or other materials to verify completeness, correctness, consistency, compliance, or authenticity. | | |

| 0854 Computer Engineering Series | | |
|---|---|---|
| **Important Competencies** | | |
| Accountability | Information Assurance | Risk Management |
| Attention to Detail | Integrity/Honesty | Self-Management |
| Communications Security Management | Interpersonal Skills | Software Development |
| Compliance | Leadership | Software Engineering |
| Computer Network Defense | Learning | Software Testing and Evaluation |
| Computer Skills | Operating Systems | Stress Tolerance |
| Creative Thinking | Oral Communication | Systems Integration |
| Customer Service | Problem Solving | Systems Testing and Evaluation |
| Data Management | Reading | Teamwork |
| Decision Making | Reasoning | Technical Competence |
| Flexibility | Requirements Analysis | Technology Awareness |
| Hardware | Resilience | Writing |
| **Important Tasks** | | |
| Recommends improvements or solutions to problems, or determines appropriate actions | | |
| Makes improvements, solves problems, or takes corrective action when problems arise | | |
| Identifies or anticipates needs or problems | | |
| Uses computer systems or applications to access, create, edit, print, send, retrieve, or manipulate data, files, or other information | | |
| Promotes or develops and maintains good working relationships with key individuals or groups | | |
| Keeps abreast of latest technology, information, research, etc., to maintain knowledge in field of expertise (for example, reads trade journals, participates in professional/technical associations, maintains credentials) | | |
| Develops and maintains relationships with customers with diverse needs | | |
| Monitors own progress on work products against assigned goals | | |
| Evaluates vendors, products, services, systems, or proposals to make recommendations for contracting (including licensing agreements) | | |
| Provides technical advice or assistance to others | | |
| Collaborates with others or works on teams to accomplish work-related activities | | |
| Gives presentations or briefings | | |

| 0391 Telecommunications Series | | |
|---|---|---|
| **Important Competencies** | | |
| Accountability | Integrity/Honesty | Reasoning |
| Attention to Detail | Interpersonal Skills | Resilience |
| Communications Security Management | Leadership | Security |
| Compliance | Learning | Self-Management |
| Computer Skills | Memory | Stress Tolerance |
| Conflict Management | Oral Communication | Teaching Others |
| Creative Thinking | Organizational Awareness | Teamwork |
| Customer Service | Partnering | Technical Competence |
| Decision Making | Physical Security | Telecommunications |
| Flexibility | Planning and Evaluating | Writing |
| Information Assurance | Problem Solving | |
| Information Management | Reading | |
| **Important Tasks** | | |
| Makes improvements, solves problems, or takes corrective action when problems arise. | | |
| Develops and maintains relationships with customers with diverse needs. | | |
| Recommends improvements or solutions to problems, or determines appropriate actions. | | |
| Identifies or anticipates needs or problems. | | |
| Promotes or develops and maintains good working relationships with key individuals or groups. | | |
| Monitors own progress on work products against assigned goals. | | |
| Uses computer systems or applications to access, create, edit, print, send, retrieve, or manipulate data, files, or other information. | | |
| Provides technical advice or assistance to others. | | |
| Enters data or other information into a computer. | | |
| Evaluates and provides feedback on others performance. | | |
| Attends briefings, meetings, conferences, or hearings. | | |
| Schedules work assignments, sets priorities, and coordinates the work of staff. | | |

# Appendix B – Cybersecurity Competencies

### General KSAs/Competencies

| | | |
|---|---|---|
| Accountability | Information Management | Political Savvy |
| Administration and Management | Integrity/Honesty | Problem Solving |
| Agility | Interpersonal Skills | Reading |
| Attention to Detail | Leadership | Reasoning |
| Computer Skills | Learning | Resilience |
| Conflict Management | Managing Human Resources | Self-Management |
| Contracting/Procurement | Mathematical Reasoning | Spatial Orientation |
| Creative Thinking | Memory | Stamina |
| Customer Service | Mental Visualization | Strategic Thinking |
| Decision Making | Oral Communication | Stress Tolerance |
| External Awareness | Organizational Awareness | Teaching Others |
| Financial Management | Partnering | Teamwork |
| Flexibility | Perceptual Speed | Technical Competence |
| Human Capital Management | Performance Management | Visual Identification |
| Influencing/Negotiating | Planning and Evaluating | Writing |

### General KSA/Competency Definitions

- **Accountability** – Holds self and others accountable for measurable high-quality, timely, and cost-effective results. Determines objectives, sets priorities, and delegates work. Accepts responsibility for mistakes. Complies with established control systems and rules.
- **Administration and Management** – Knowledge of planning, coordination, and execution of business functions, resource allocation, and production.
- **Agility** – Bends, stretches, twists, or reaches out with the body, arms, or legs.
- **Attention to Detail** – Is thorough when performing work and conscientious about attending to detail.
- **Computer Skills** – Uses computers, software applications, databases, and automated systems to accomplish work.
- **Conflict Management** – Manages and resolves conflicts, grievances, confrontations, or disagreements in a constructive manner to minimize negative personal impact.
- **Contracting/Procurement** – Knowledge of various types of contracts, techniques, or requirements (for example, Federal Acquisitions Regulations) for contracting or procurement, and contract negotiation and administration.
- **Creative Thinking** – Uses imagination to develop new insights into situations and applies innovative solutions to problems; designs new methods where established methods and procedures are inapplicable or are unavailable.
- **Customer Service** – Works with clients and customers (that is, any individuals who use or receive the services or products that your work unit produces, including the general public, individuals who work in the agency, other agencies, or organizations outside the

Government) to assess their needs, provide information or assistance, resolve their problems, or satisfy their expectations; knows about available products and services; is committed to providing quality products and services.

- **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; causes change.
- **External Awareness** – Identifies and understands economic, political, and social trends that affect the organization.
- **Financial Management** – Prepares, justifies, and/or administers the budget for program areas; plans, administers, and monitors expenditures to ensure cost-effective support of programs and policies; assesses financial condition of an organization.
- **Flexibility** – Is open to change and new information; adapts behavior or work methods in response to new information, changing conditions, or unexpected obstacles; effectively deals with ambiguity.
- **Human Capital Management** – Builds and manages workforce based on organizational goals, budget considerations, and staffing needs. Ensures that employees are appropriately recruited, selected, appraised, and rewarded; takes action to address performance problems. Manages a multi-sector workforce and a variety of work situations.
- **Influencing/Negotiating** – Persuades others to accept recommendations, cooperate, or change their behavior; works with others towards an agreement; negotiates to find mutually acceptable solutions.
- **Information Management** – Identifies a need for and knows where or how to gather information; organizes and maintains information or information management systems.
- **Integrity/Honesty** – Contributes to maintaining the integrity of the organization; displays high standards of ethical conduct and understands the impact of violating these standards on an organization, self, and others; is trustworthy.
- **Interpersonal Skills** – Shows understanding, friendliness, courtesy, tact, empathy, concern, and politeness to others; develops and maintains effective relationships with others; may include effectively dealing with individuals who are difficult, hostile, or distressed; relates well to people from varied backgrounds and different situations; is sensitive to cultural diversity, race, gender, disabilities, and other individual differences.
- **Leadership** – Influences, motivates, and challenges others; adapts leadership styles to a variety of situations.
- **Learning** – Uses efficient learning techniques to acquire and apply new knowledge and skills; uses training, feedback, or other opportunities for self-learning and development.
- **Managing Human Resources** – Plans, distributes, coordinates, and monitors work assignments of others; evaluates work performance and provides feedback to others on their performance; ensures that staff are appropriately selected, utilized, and developed, and that they are treated in a fair and equitable manner.
- **Mathematical Reasoning** – Solves practical problems by choosing appropriately from a variety of mathematical and statistical techniques.
- **Memory** – Recalls information that has been presented previously.
- **Mental Visualization** – Sees things in the mind by mentally organizing and processing symbols, pictures, graphs, objects, or other information (for example, sees a building from a blueprint, or sees the flow of work activities from reading a work plan).

- **Oral Communication** – Expresses information (for example, ideas or facts) to individuals or groups effectively, taking into account the audience and nature of the information (for example, technical, sensitive, controversial); makes clear and convincing oral presentations; listens to others, attends to nonverbal cues, and responds appropriately.
- **Organizational Awareness** – Knows the organization's mission and functions, and how its social, political, and technological systems work and operates effectively within them; this includes the programs, policies, procedures, rules, and regulations of the organization.
- **Partnering** – Develops networks and builds alliances; collaborates across boundaries to build strategic relationships and achieve common goals.
- **Perceptual Speed** – Quickly and accurately sees detail in words, numbers, pictures, and graphs.
- **Performance Management** – Knowledge of performance management concepts, principles, and practices related to planning, monitoring, rating, and rewarding employee performance.
- **Planning and Evaluating** – Organizes work, sets priorities, and determines resource requirements; determines short- or long-term goals and strategies to achieve them; coordinates with other organizations or parts of the organization to accomplish goals; monitors progress and evaluates outcomes.
- **Political Savvy** – Identifies the internal and external politics that impact the work of the organization. Perceives organizational and political reality and acts accordingly.
- **Problem Solving** – Identifies problems; determines accuracy and relevance of information; uses sound judgment to generate and evaluate alternatives, and to make recommendations.
- **Reading** – Understands and interprets written material, including technical material, rules, regulations, instructions, reports, charts, graphs, or tables; applies what is learned from written material to specific situations.
- **Reasoning** – Identifies rules, principles, or relationships that explain facts, data, or other information; analyzes information and makes correct inferences or draws accurate conclusions.
- **Resilience** – Deals effectively with pressure; remains optimistic and persistent, even under adversity. Recovers quickly from setbacks.
- **Self-Management** – Sets well-defined and realistic personal goals; displays a high level of initiative, effort, and commitment towards completing assignments in a timely manner; works with minimal supervision; is motivated to achieve; demonstrates responsible behavior.
- **Spatial Orientation** – Knows one's location in relation to the environment; determines where other objects are in relation to one's self (for example, when using a map).
- **Stamina** – Exerts oneself physically over long periods of time without tiring (which may include performing repetitive tasks such as data entry or coding).
- **Strategic Thinking** – Formulates effective strategies consistent with the business and competitive strategy of the organization in a global economy; examines policy issues and strategic planning with a long-term perspective; determines objectives and sets priorities; anticipates potential threats or opportunities.

- **Stress Tolerance** – Deals calmly and effectively with high stress situations (for example, tight deadlines, hostile individuals, emergency situations, dangerous situations).
- **Teaching Others** – Helps others learn through formal or informal methods; identifies training needs; provides constructive feedback; coaches others on how to perform tasks; acts as a mentor.
- **Teamwork** – Encourages and facilitates cooperation, pride, trust, and group identity; fosters commitment and team spirit; works with others to achieve goals.
- **Technical Competence** – Uses knowledge that is acquired through formal training or extensive on-the-job experience to perform one's job; works with, understands, and evaluates technical information related to the job; advises others on technical issues.
- **Visual Identification** – Accurately identifies people, animals, or objects based on knowledge of their characteristics.
- **Writing** – Recognizes or uses correct English grammar, punctuation, and spelling; communicates information (for example, facts, ideas, or messages) in a succinct and organized manner; produces written information, which may include technical material that is appropriate for the intended audience.

## Technical KSAs/Competencies

| | | |
|---|---|---|
| Accessibility | Forensics | Organizational Development |
| Business Processing Engineering | Hardware | Personnel Security and Safety |
| Capacity Management | Hardware Engineering | Physical Security |
| Capital Planning and Investment Assessment | Human Factors | Process Control |
| Communications Security Management | Identity Management | Product Evaluation |
| Compliance | Incident Management | Project Management |
| Computer Forensics | Information Assurance | Public Safety and Security |
| Computer Languages | Information Resources Strategy and Planning | Quality Assurance |
| Computer Network Defense | Information Systems Security Certification | Requirements Analysis |
| Computers and Electronics | Information Systems/Network Security | Risk Management |
| Configuration Management | Information Technology Architecture | Security |
| Cost-Benefit Analysis | Information Technology Performance Assessment | Software Development |
| Criminal Investigation | Information Technology Research and Development | Software Engineering |
| Criminal Law | Infrastructure Design | Software Testing and Evaluation |
| Data Management | Internal Controls | Surveillance |
| Database Administration | Knowledge Management | Systems Integration |
| Database Management Systems | Legal, Government and Jurisprudence | Systems Life Cycle |
| Distributed Systems | Logical Systems Design | Systems Testing and Evaluation |
| Economics and Accounting | Modeling and Simulation | Technical Documentation |
| Electronic Commerce (e-Commerce) | Multimedia Technologies | Technology Awareness |
| Embedded Computers | Network Management | Telecommunications |
| Encryption | Object Technology | Vulnerabilities Assessment |
| Engineering and Technology | Operating Systems | Web Technology |
| Enterprise Architecture | Operations Support | |

## Technical KSA/Competency Definitions

- **Accessibility** – Knowledge of tools, equipment, and technologies used to help individuals with disabilities use computer equipment and software.
- **Business Process Reengineering** – Knowledge of methods, metrics, tools, and techniques of Business Process Reengineering.

- **Capacity Management** – Knowledge of the principles and methods for monitoring, estimating, or reporting actual performance or the performance capability of information systems or components.
- **Capital Planning and Investment Assessment** – Knowledge of the principles and methods of capital investment analysis or business case analysis, including return on investment analysis.
- **Communications Security Management** – Knowledge of the principles, policies, and procedures involved in ensuring the security of communications services and data, and in maintaining the communications environment on which it resides.
- **Compliance** – Knowledge of procedures for assessing, evaluating, and monitoring programs or projects for compliance with Federal laws, regulations, and guidance.
- **Computer Forensics** – Knowledge of tools and techniques used in data recovery and preservation of electronic evidence.
- **Computer Languages** – Knowledge of computer languages and their applications to enable a system to perform specific functions.
- **Computer Network Defense** – Knowledge of defensive measures to detect, respond, and protect information, information systems, and networks from threats.
- **Computers and Electronics** – Knowledge of electric circuit boards, processors, chips, and computer hardware and software, including applications and programming.
- **Configuration Management** – Knowledge of the principles and methods for planning or managing the implementation, update, or integration of information systems components.
- **Cost-Benefit Analysis** – Knowledge of the principles and methods of cost-benefit analysis, including the time value of money, present value concepts, and quantifying tangible and intangible benefits.
- **Criminal Investigation** – Knowledge of the guidelines, regulations, and procedures associated with criminal investigation, including evidence detection and handling and drawing appropriate factual inferences and conclusions.
- **Criminal Law** – Knowledge of state and Federal criminal laws, including procedures, regulations, guidelines, and precedents related to admissibility of evidence and prosecution.
- **Data Management** – Knowledge of the principles, procedures, and tools of data management, such as modeling techniques, data backup, data recovery, data dictionaries, data warehousing, data mining, data disposal, and data standardization processes.
- **Database Administration** – Knowledge of the principles, methods, and tools for automating, developing, implementing, or administering database systems.
- **Database Management Systems** – Knowledge of the uses of database management systems and software to control the organization, storage, retrieval, security, and integrity of data.
- **Distributed Systems** – Knowledge of the principles, theoretical concepts, and tools underlying distributed computing systems, including their associated components and communication standards.
- **Economics and Accounting** – Knowledge of economic and accounting principles and practices, tax law and practices, the financial markets, banking, and the analysis and reporting of financial data.

- **Electronic Commerce (e-Commerce) –** Knowledge of the principles, methods, and tools for conducting business online, including electronic data interchange.
- **Embedded Computers** – Knowledge of specifications and uses of specialized computer systems used to control devices (for example, automobiles, helicopters), including the appropriate programming languages.
- **Encryption** – Knowledge of procedures, tools, and applications used to keep data, or information secure, including public key infrastructure, point-to-point encryption, and smart cards.
- **Engineering and Technology** – Knowledge of engineering concepts, principles, and practices, and of equipment, tools, mechanical devices, and their uses to produce motion, light, power, technology, and other applications.
- **Enterprise Architecture** – Knowledge of principles, concepts, and methods of enterprise architecture to align information technology (IT) strategy, plans, and systems with the mission, goals, structure, and processes of the organization.
- **Forensics** – Knowledge of procedures of civil, criminal, or administrative hearings, evidence collection, including the delivery and receipt of evidence, classes of evidence, and rules of evidence and legal procedures.
- **Hardware** – Knowledge of specifications, uses, and types of computer or computer-related equipment.
- **Hardware Engineering** – Knowledge of the principles, methods, and tools for designing, developing, and testing computer or computer-related equipment.
- **Human Factors** – Knowledge of the principles, methods, and tools used to identify and apply information about human behavior, abilities, limitations, and other characteristics to the design of tools, machines, systems, tasks, jobs, and environments for effective human use.
- **Identity Management** – Knowledge of methods and controls to validate the identity of individuals to verify access approval and level, and monitor activity to ensure that only authorized access is taking place.
- **Incident Management** – Knowledge of the tactics, technologies, principles, and processes to protect, analyze, prioritize, and handle incidents.
- **Information Assurance** – Knowledge of methods and procedures to protect information systems and data by ensuring their availability, authentication, confidentiality, and integrity.
- **Information Resources Strategy and Planning** – Knowledge of the principles, methods, and techniques of IT assessment, planning, management, monitoring, and evaluation, such as IT baseline assessment, interagency functional analysis, contingency planning, and disaster recovery.
- **Information Systems Security Certification** – Knowledge of the principles, methods, and tools for evaluating information systems security features against a set of specified security requirements. Includes developing security certification and accreditation plans and procedures, documenting deficiencies, reporting corrective actions, and recommending changes to improve the security of information systems.
- **Information Systems/Network Security** – Knowledge of methods, tools, and procedures, including development of information security plans, to prevent information systems vulnerabilities, and provide or restore security of information systems and network services.

- **Information Technology Architecture** – Knowledge of architectural methodologies used in the design and development of information systems, including the physical structure of a system's internal operations and interactions with other systems.
- **Information Technology Performance Assessment** – Knowledge of the principles, methods, and tools (for example, surveys, system performance measures) to assess the effectiveness and practicality of IT systems.
- **Information Technology Research and Development** – Knowledge of scientific principles, methods, and tools of basic and applied research used to conduct a systematic inquiry into a subject matter area.
- **Infrastructure Design** – Knowledge of the architecture and topology of software, hardware, and networks, including LANS, WANS, and telecommunications systems, their components and associated protocols and standards, and how they operate and integrate with one another and with associated controlling software.
- **Internal Controls** – Knowledge of the principles, methods, and techniques for establishing internal control activities (for example, authorizations, verifications, reconciliations), monitoring their use, and evaluating their performance (for example, identification of material weaknesses or significant deficiencies).
- **Knowledge Management** – Knowledge of the value of collected information and the methods of sharing that information throughout an organization.
- **Legal, Government and Jurisprudence** – Knowledge of laws, legal codes, court procedures, precedents, legal practices and documents, government regulations, executive orders, agency rules, government organization and functions, and the democratic political process.
- **Logical Systems Design** – Knowledge of the principles and methods for designing business logic components, system processes and outputs, user interfaces, data inputs, and productivity tools (for example, computer-aided software engineering).
- **Modeling and Simulation** – Knowledge of mathematical modeling and simulation tools and techniques to plan and conduct test and evaluation programs, characterize systems support decisions involving requirements, evaluate design alternatives, or support operational preparation.
- **Multimedia Technologies** – Knowledge of the principles, methods, tools, and techniques to develop or apply technology using text, audio, graphics, or other media.
- **Network Management** – Knowledge of the operation, management, and maintenance of network and telecommunication systems and linked systems and peripherals.
- **Object Technology** – Knowledge of the principles, methods, tools, and techniques that use object-oriented languages, analysis, and design methodologies.
- **Operating Systems** – Knowledge of computer network, desktop, and mainframe operating systems and their applications.
- **Operations Support** – Knowledge of procedures to ensure production or delivery of products and services, including tools and mechanisms for distributing new or enhanced software.
- **Organizational Development** – Knowledge of the principles of organizational development and change management theories, and their applications.
- **Personnel Security and Safety** – Knowledge of methods and controls of personnel, public safety, and security operations; investigation and inspection techniques; or rules,

regulations, precautions, and prevention techniques for the protection of people, data, or property.

- **Physical Security** – Knowledge of methods and controls to protect an organization from natural or man-made threats to physical locations where information systems equipment is located or work is performed (for example, computer rooms, work locations, and equipment rooms).
- **Process Control** – Knowledge of the principles, methods, and procedures used for the automated control of a process, including the design, development, and maintenance of associated software, hardware, and systems.
- **Product Evaluation** – Knowledge of methods for researching and analyzing external products to determine their potential for meeting organizational standards and business needs.
- **Project Management** – Knowledge of the principles, methods or tools for developing, scheduling, coordinating, and managing projects and resources, including monitoring and inspecting costs, work, and contractor performance.
- **Public Safety and Security** – Knowledge of military, weaponry, and intelligence operations; public safety and security operations; occupational health and safety; investigation and inspection techniques; or rules, regulations, precautions, and prevention techniques for the protection of people, data, and property.
- **Quality Assurance** – Knowledge of the principles, methods, and tools of quality assurance and quality control used to ensure a product fulfills functional requirements and standards.
- **Requirements Analysis** – Knowledge of the principles and methods to identify, analyze, specify, design, and manage functional and infrastructure requirements; includes translating functional requirements into technical requirements used for logical design or presenting alternative technologies or approaches.
- **Risk Management** – Knowledge of the principles, methods, and tools used for risk assessment and mitigation, including assessment of failures and their consequences.
- **Security** – Knowledge of the laws, regulations, and guidelines related to securing personnel, facilities, and information, including the requirements for handling, transporting, and protecting classified information and proper reporting of security incidents.
- **Software Development** – Knowledge of the principles, methods, and tools for designing, developing, and testing software in a given environment.
- **Software Engineering** – Knowledge of software engineering design and development methodologies, paradigms, and tools; the software life cycle; software reusability; and software reliability metrics.
- **Software Testing and Evaluation** – Knowledge of the principles, methods, and tools for analyzing and developing software test and evaluation procedures.
- **Surveillance** – Knowledge of surveillance and counter-surveillance techniques, policies, and laws, including overt and covert methods and electronic, optical, and video surveillance methods and tools.
- **Systems Integration** – Knowledge of the principles, methods, and procedures for installing, integrating, and optimizing information systems components.
- **Systems Life Cycle** – Knowledge of systems life cycle management concepts used to plan, develop, implement, operate, and maintain information systems.

- **Systems Testing and Evaluation** – Knowledge of the principles, methods, and tools for analyzing and developing systems test and evaluation procedures and technical characteristics of IT systems, including identifying critical operational issues.
- **Technical Documentation** – Knowledge of procedures for developing technical and operational support documentation.
- **Technology Awareness** – Knowledge of developments and new applications of IT (hardware, software, telecommunications), emerging technologies and their applications to business processes, and applications and implementation of information systems to meet organizational requirements.
- **Telecommunications** – Knowledge of transmissions, broadcasting, switching, control, and operation of telecommunications systems.
- **Vulnerabilities Assessment** – Knowledge of the principles, methods, and tools for assessing vulnerabilities, and developing or recommending appropriate mitigation countermeasures.
- **Web Technology** – Knowledge of the principles and methods of web technologies, tools, and delivery systems, including web security, privacy policy practices, and user interface issues.

**Note:** Additional technical competencies should be identified based on the specific occupation.


**U.S. Office of Personnel Management**
**Employee Services**
1900 E Street, NW, Washington, DC 20415
**OPM**.GOV

ES-03225-10/2018