

## OPM Cybersecurity Codes Linked to the NICE Cybersecurity Workforce Framework

Table 1: Work Role Descriptions and New Cybersecurity Codes

Category	Specialty Area	Work Role	OPM Code	Work Role Description
Securely Provision	Risk Management	Authorizing Official/Designating Representative	611	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	612	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	Software Developer	621	Develops, creates, maintains, and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs.
		Secure Software Assessor	622	Analyzes the security of new or existing computer applications, software, or specialized utility programs and provides actionable results.
	Systems Architecture	Enterprise Architect	651	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	652	Designs enterprise and systems security throughout the development life cycle; translates technology and environmental conditions (e.g., law and regulation) into security designs and processes.

Category	Specialty Area	Work Role	OPM Code	Work Role Description
	Technology R&D	Research & Development Specialist	661	Conducts software and systems engineering and software systems research in order to develop new capabilities, ensuring cybersecurity is fully integrated. Conducts comprehensive technology research to evaluate potential vulnerabilities in cyberspace systems.
	Systems Requirements Planning	Systems Requirements Planner	641	Consults with customers to evaluate functional requirements and translate functional requirements into technical solutions.
	Test and Evaluation	System Testing and Evaluation Specialist	671	Plans, prepares, and executes tests of systems to evaluate results against specifications and requirements as well as analyze/report test results.
	Systems Development	Information Systems Security Developer	631	Designs, develops, tests, and evaluates information system security throughout the systems development life cycle.
		Systems Developer	632	Designs, develops, tests, and evaluates information systems throughout the systems development life cycle.
Operate and Maintain	Data Administration	Database Administrator	421	Administers databases and/or data management systems that allow for the storage, query, and utilization of data.
		Data Analyst	422	Examines data from multiple disparate sources with the goal of providing new insight. Designs and implements custom algorithms, flow processes, and layouts for complex, enterprise-scale data sets used for modeling, data mining, and research purposes.
	Knowledge Management	Knowledge Manager	431	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	Technical Support Specialist	411	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).

Category	Specialty Area	Work Role	OPM Code	Work Role Description
	Network Services	Network Operations Specialist	441	Plans, implements, and operates network services/systems, to include hardware and virtual environments.
	Systems Administration	System Administrator	451	Installs, configures, troubleshoots, and maintains hardware and software, and administers system accounts.
	Systems Analysis	Systems Security Analyst	461	Responsible for the analysis and development of the integration, testing, operations, and maintenance of systems security.
Oversee and Govern	Legal Advice and Advocacy	Cyber Legal Advisor	731	Provides legal advice and recommendations on relevant topics related to cyber law.
		Privacy Compliance Manager	732	Develops and oversees privacy compliance program and privacy program staff, supporting privacy compliance needs of privacy and security executives and their teams.
	Training, Education, and Awareness	Cyber Instructional Curriculum Developer	711	Develops, plans, coordinates, and evaluates cyber training/education courses, methods, and techniques based on instructional needs.
		Cyber Instructor	712	Develops and conducts training or education of personnel within cyber domain.
	Cybersecurity Management	Information Systems Security Manager	722	Responsible for the cybersecurity of a program, organization, system, or enclave.
		COMSEC Manager	723	Manages the Communications Security (COMSEC) resources of an organization (CNSSI 4009).
	Strategic Planning and Policy	Cyber Workforce Developer and Manager	751	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	752	Develops cyberspace plans, strategy and policy to support and align with organizational cyberspace missions and initiatives.

Category	Specialty Area	Work Role	OPM Code	Work Role Description
	Executive Cyber Leadership	Executive Cyber Leadership	901	Executes decision-making authorities and establishes vision and direction for an organization's cyber and cyber-related resources and/or operations.
	Acquisition and Program/Project Management	Program Manager	801	Leads, coordinates, communicates, integrates and is accountable for the overall success of the program, ensuring alignment with critical agency priorities.
		IT Project Manager	802	Directly manages information technology projects to provide a unique service or product.
		Product Support Manager	803	Manages the package of support functions required to field and maintain the readiness and operational capability of systems and components.
		IT Investment/Portfolio Manager	804	Manages a portfolio of IT capabilities that align with the overall needs of mission and business enterprise priorities.
		IT Program Auditor	805	Conducts evaluations of an IT program or its individual components, to determine compliance with published standards.
Protect and Defend	Cyber Defense Analysis	Cyber Defense Analyst	511	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.
	Cyber Defense Infrastructure Support	Cyber Defense Infrastructure Support Specialist	521	Tests, implements, deploys, maintains, and administers the infrastructure hardware and software.
	Incident Response	Cyber Defense Incident Responder	531	Investigates, analyzes, and responds to cyber incidents within the network environment or enclave.
	Vulnerability Assessment and Management	Vulnerability Assessment Analyst	541	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.

Category	Specialty Area	Work Role	OPM Code	Work Role Description
Analyze	Threat Analysis	Warning Analyst	141	Develops unique cyber indicators to maintain constant awareness of the status of the highly dynamic operating environment. Collects, processes, analyzes, and disseminates cyber warning assessments.
	Exploitation Analysis	Exploitation Analyst	121	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	All-Source Analyst	111	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	112	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	Target Developer	131	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	132	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.

Category	Specialty Area	Work Role	OPM Code	Work Role Description
	Language Analysis	Multi-Disciplined Language Analyst	151	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	Collection Operations	All Source-Collection Manager	311	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	312	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	Cyber Intel Planner	331	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.

Category	Specialty Area	Work Role	OPM Code	Work Role Description
		Cyber Ops Planner	332	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	333	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	Cyber Operator	321	Conducts collection, processing, and/or geolocation of systems in order to exploit, locate, and/or track targets of interest. Performs network navigation, tactical forensic analysis, and, when directed, executing on-net operations.
Investigate	Cyber Investigation	Cyber Crime Investigator	221	Identifies, collects, examines, and preserves evidence using controlled and documented analytical and investigative techniques.
	Digital Forensics	Forensics Analyst	211	Conducts deep-dive 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	212	Analyzes digital evidence and investigates computer security incidents to derive useful information in support of system/network vulnerability mitigation.
Not Applicable	Not Applicable	Not Applicable	000	Does NOT involve work functions in information technology (IT), cybersecurity, or cyber-related areas.