

Activity Area/Work Category	Common Title or Work Role	NICE ID	NOC	Major Cybersecurity Responsibility (NICE and other sources)	Key Cybersecurity Competencies
Oversee & Govern	CEO/Senior Leadership/Owner	OV-EXL-001	0012,0013	Executes decision-making authorities and establishes vision and direction for an organization's cyber and cyber-related resources and/or operations.	Strategic cyber planning Business & threat context Risk management Cyber legal and policy context Cyber compliance requirements Cybersecurity controls (management, operational, technical) Cybersecurity program management
	Chief Information Officer/Chief Technical Officer	None	0012, 0013, 0211, 0213	Leads and executes decision-making authorities related to organizational IT, infrastructure and technical services. This often includes cybersecurity services.	Strategic cyber planning Business & threat context Risk management Cyber legal and policy context Cyber compliance requirements Cybersecurity controls (management, operational, technical) Cybersecurity program management Cybersecurity assessment and measurement
	Cyber Legal Advisor	OV-LGA-001	4112, 4211	Provides legal advice and recommendations on relevant topics related to cyber law.	Cyber legal and policy context Cyber compliance requirements Threat context
	Privacy Officer/Privacy Compliance Manager	OV-LGA-002	0213	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.	Cyber legal and policy context Cyber compliance requirements Threat context Privacy relevant security controls
	Communications Security (COMSEC) Manager	OV-MGT-002	0131, 0213	Individual who manages the Communications Security (COMSEC) resources of an	Security program management BCP/DRP Supply chain risk management

Activity Area/Work Category	Common Title or Work Role	NICE ID	NOC	Major Cybersecurity Responsibility (NICE and other sources)	Key Cybersecurity Competencies
				organization (CNSSI 4009) or key custodian for a Crypto Key Management System (CKMS).	COMSEC policies, guidelines and management requirements COMSEC accounting Encryption/PKI infrastructure and applications COMSEC incident management
	Cyber Workforce Developer and Manager	OV-SPP-001	4156	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.	Cybersecurity career paths Cybersecurity labour market information and sources Cybersecurity occupational standards Cybersecurity certifications and accreditations Assessing cybersecurity competencies
	Cyber Instructional Curriculum Developer	OV-TEA-001	4011, 4021, 4216	Develops, plans, coordinates, and evaluates cyber training/education courses, methods, and techniques based on instructional needs.	Relevant cyber domain knowledge (topic-based) Assessing cybersecurity competencies
	Cyber Instructor	OV-TEA-002	4011, 4021, 4216	Develops and conducts training or education of personnel within cyber domain.	Relevant cyber domain knowledge (topic-based) Assessing cybersecurity competencies
	Cyber Policy and Strategy Planner	OV-SPP-002	0412, 4161	Develops and maintains cybersecurity plans, strategy, and policy to support and align with organizational cybersecurity initiatives and regulatory compliance.	Cybersecurity program management BCP/DRP Cyber legal and policy context Business & threat context Cyber policy planning & development Cybersecurity controls (management, operational, technical)
	Program Manager	OV-PMA-001	0012, 0013, 0211	Leads, coordinates, communicates, integrates, and is accountable for the overall success of the program,	Cybersecurity risk management Business and threat context Cybersecurity program management

Activity Area/Work Category	Common Title or Work Role	NICE ID	NOC	Major Cybersecurity Responsibility (NICE and other sources)	Key Cybersecurity Competencies
				ensuring alignment with agency or enterprise priorities.	BCP/DRP Supply chain risk management Cyber maturity models Cybersecurity standards Cybersecurity assessment and measurement
	IT Project Manager	OV-PMA-002	0211, 0213	Directly manages information technology projects.	Threat and risk assessment Cybersecurity risk management Business and threat context Technical context Cyber systems integration Cybersecurity project management Cyber procurement requirements Supply chain risk management Cybersecurity standards Cybersecurity assessment and measurement Cybersecurity controls (management, operational, technical)
	Product Support Manager	OV-PMA-003	0211, 0213	Manages the package of support functions required to field and maintain the readiness and operational capability of systems and components.	Threat and risk assessment Cybersecurity risk management Business and threat context Technical context Cyber systems integration Cybersecurity project management Supply chain risk management Cybersecurity standards Cybersecurity controls (management, operational, technical) Cybersecurity product testing and evaluation processes Cybersecurity product lifecycle management

Activity Area/Work Category	Common Title or Work Role	NICE ID	NOC	Major Cybersecurity Responsibility (NICE and other sources)	Key Cybersecurity Competencies
	IT Investment/Portfolio Manager	OV-PMA-004	0211, 0213	Manages a portfolio of IT investments that align with the overall needs of mission and enterprise priorities.	Cybersecurity risk management Business and threat context Cybersecurity program management Supply chain risk management Cyber maturity models Cybersecurity standards Cybersecurity assessment and measurement Cybersecurity product lifecycle management
	IT Program Auditor	OV-PMA-005	0211, 0213	Conducts evaluations of an IT program or its individual components to determine compliance with published standards.	Cybersecurity audit policies, practices and procedures Threat and risk assessment Cybersecurity risk management Business and threat context Technical context Legal and policy context Compliance requirements Cyber procurement requirements Supply chain risk management Cybersecurity standards Cybersecurity assessment and measurement Cybersecurity controls (management, operational, technical) Vulnerability assessment Cybersecurity testing and evaluation processes
	Business Analyst	None	1122, 2171, 4162	Analyzes and identifies needs, recommends solutions that deliver business value to stakeholders.	Cybersecurity governance, roles and responsibilities Cybersecurity risk management Business and threat context Technical context Legal and policy context Compliance requirements

Activity Area/Work Category	Common Title or Work Role	NICE ID	NOC	Major Cybersecurity Responsibility (NICE and other sources)	Key Cybersecurity Competencies
					<ul style="list-style-type: none"> Cyber procurement requirements Supply chain risk management Cybersecurity standards Cybersecurity assessment and measurement Cybersecurity controls (management, operational, technical) Vulnerability assessment Cybersecurity testing and evaluation processes
	Financial Analyst	None	1112	Collects and analyzes financial information and risks. Provides related financial estimates, forecasts and trends. Provides advice to support financial and investment activities.	<ul style="list-style-type: none"> Cybersecurity risk management Business and threat context Legal, policy and financial context Cybersecurity program requirements Cybersecurity procurement and acquisition Cybersecurity assessment and measurement
	Risk Analyst	None	1112, 4162	Collects and analyzes organizational risks. Provides related risk assessments and advice on mitigations.	<ul style="list-style-type: none"> Cybersecurity risk management Threat and risk assessment methodologies Business and threat context Legal, policy and financial context Cybersecurity program requirements
	Communications Specialist	None	0124, 1123	Plan, organize, and develop advertising, marketing and public relations.	<ul style="list-style-type: none"> Cyber threat context Legal and policy context Compliance requirements BCP/DRP Communications during a cyber incident (crisis communications)
	Webmaster/Online Communications Manager	None	2175	Researches, designs, develops and produces Internet and Intranet sites and web-based media.	<ul style="list-style-type: none"> Cybersecurity threats Web application vulnerabilities Software testing and evaluation

Activity Area/Work Category	Common Title or Work Role	NICE ID	NOC	Major Cybersecurity Responsibility (NICE and other sources)	Key Cybersecurity Competencies
					Cybersecurity incident response requirements
	Learning and Development Specialist	None	4011, 4021, 4216	Develops, plans, coordinates, and evaluates organizational and individual learning and development programs and activities	Organizational cybersecurity requirements Cybersecurity roles and responsibilities Cybersecurity career pathways Assessing cybersecurity competencies
	Business Continuity/ Resiliency Planner	None	1112, 2171	Identify, coordinate and oversee development of a business continuity plan to support organizational resilience to fraud, financial crime, cyber-attack, terrorism, and infrastructure failure.	Threat and risk assessment Cybersecurity risk management Business and threat context Technical context Organizational cybersecurity requirements Cybersecurity roles and responsibilities Cybersecurity plans, processes and procedures Cybersecurity incident management Cybersecurity controls (management, operational, technical)
	Procurement Specialist	None	1225	Identify and acquire general and specialized equipment, materials, land or access rights and business services for use or for further processing by their organization.	Threat and risk assessment Cybersecurity risk management Business and threat context Technical context Cybersecurity project management Supply chain risk management Cybersecurity standards Cybersecurity controls (management, operational, technical)

Activity Area/Work Category	Common Title or Work Role	NICE ID	NOC	Major Cybersecurity Responsibility (NICE and other sources)	Key Cybersecurity Competencies
					Cybersecurity product testing and evaluation processes Cybersecurity product lifecycle management
Design & Develop (Securely Provision in the NICE)	Authorizer (often CIO or system owner)	SP-RSK-001	0012/0013/0211	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).	Strategic cyber planning Business & threat context Risk management Cyber legal and policy context Cyber compliance requirements Cybersecurity controls (management, operational, technical) Cybersecurity program management Cybersecurity assessment and measurement
	Enterprise Architect	SP-ARC-001	0211/2147	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.	Organizational cyber goals Cybersecurity architecture and design Cybersecurity engineering Threat and risk assessment Cyber legal and policy context Cyber compliance requirements Cybersecurity controls (management, operational, technical) Cyber systems integration Encryption/PKI
	Software Developer	SP-DEV-001	2241/2233/2243	Develops, creates, maintains, and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs.	System and software vulnerabilities Software security testing and evaluation Software security tools, techniques and procedures Vulnerability assessment and penetration testing practices and tools