Annex B – National Security and Law Enforcement Cybersecurity Roles

As previously noted, the following provides a summary of the cybersecurity roles that are typically employed within national security, military, intelligence and law enforcement occupations. Not commonly found within the broader Canadian labour market, these are direct excerpts from the U.S. NICE supplement that list work roles and tasks.

Notably, individuals who fulfill these roles typically drawn from the larger labour pool based upon related experience and evidence of suitable competencies, then they participate in domain specific training and education through the employer. For example, those employed in technical roles, such as Exploitation Analyst or Cyber Operator, are often drawn from the Protect & Defend activity area/work categories or provided training and education to support their added responsibilities with their organization (e.g. military, intelligence, policing, etc.).

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.	AN-TWA-001
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.	AN-EXP-001
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.	AN-ASA-001

	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.	AN-ASA-002
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.	AN-TGT-001
	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.	AN-TGT-002
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.	AN-LNG-001

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.	CO-CLO-001
	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.	CO-CLO-002
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.	CO-OPL-001

	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.	CO-OPL-002
	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.	CO-OPL-003
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.	CO-OPS-001
Investigate (IN)			
Cyber Investigation (INV)	Cyber Crime Investigator	Identifies, collects, examines, and preserves evidence using controlled and documented analytical and investigative techniques.	IN-INV-001

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.	IN-FOR-001
	Cyber Defense Forensics Analyst	Analyzes digital evidence and investigates computer security incidents to derive useful information in support of system/network vulnerability mitigation.	IN-FOR-002

Annex C – Cybersecurity Adjacent Roles within Organizations

In conjunction with the **core** roles that define the cybersecurity occupation discussed in this NOS, there are a number of **adjacent** roles that have cybersecurity responsibilities which typically form only part of their overall responsibilities within an organization. While often only employed in cybersecurity in a part-time capacity, the scope and extent to which they perform these roles will vary based on organizational size, type and degree of IT/Internet enabled infrastructure. For example, for larger IT enabled organizations, all of the following roles may apply. For smaller organizations that are not overly reliant on IT or internet connectivity for the conduct of their business, it is likely that a majority of the technical expertise and services will be outsourced. Accordingly, the remaining non-technical cybersecurity responsibilities will be distributed within the organization.

This table briefly outline common cybersecurity adjacent roles[10], the related NICE ID if applicable, the associated NOC and the main cybersecurity responsibilities. Assuming that the majority of individuals in such roles already have the required competencies for their primary roles and functions, only cybersecurity functions are provided with key competencies.[11] Specifically, for the existing workforce community and, in particular, educators, these should guide discussion around adapting training and education programs to more closely reflect the cybersecurity realities of the Canadian labour market.

[10] Other roles will be added as they are identified or emerge and follow the NOS update process outlined in the *Review and Revision* section presented earlier in this document.

[11] The prefix ‘cyber’ connotes a specialization in the cyber domain, but all positions below are assumed to have required competencies to support their primary organizational function. For example, a Cyber Instructor is assumed to have all competencies to support instruction in addition to cyber domain knowledge/experience.

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
					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.	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.	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.	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.	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

Activity Area/Work Category	Common Title or Work Role	NICE ID	NOC	Major Cybersecurity Responsibility (NICE and other sources)	Key Cybersecurity Competencies
					Identity, credentials and authentication
	Systems Requirements Planner	SP-SRP-001	2147/2171/2261	Consults with customers to evaluate functional requirements and translate functional requirements into technical solutions	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 Cybersecurity standards Cybersecurity assessment and measurement Cybersecurity product lifecycle management Identity, credentials and authentication
	System Testing and Evaluation Specialist	SP-TST-001	2173/2171/2174/2283	Plans, prepares, and executes tests of systems to evaluate results against specifications and requirements as well as analyze/report test results.	System and software vulnerabilities System and software security testing and evaluation Software security tools, techniques and procedures Vulnerability assessment and penetration testing practices and tools Cybersecurity standards Cybersecurity assessment and measurement
	Systems Developer	SP-SYS-002	2147/2173/2174	Designs, develops, tests, and evaluates information systems throughout the systems development life cycle.	Cybersecurity architecture and design Cybersecurity engineering Threat and risk assessment

Activity Area/Work Category	Common Title or Work Role	NICE ID	NOC	Major Cybersecurity Responsibility (NICE and other sources)	Key Cybersecurity Competencies
🟥					Cyber legal and policy context Cyber compliance requirements Cybersecurity controls (management, operational, technical) Cyber systems integration Encryption/PKI Cybersecurity standards Cybersecurity assessment and measurement Cybersecurity product lifecycle management Identity, credentials and authentication
🟥	Web Developer	None	2175	Researches, designs, develops and produces Internet and Intranet sites and web-based media.	Cybersecurity threats Web application vulnerabilities Software testing and evaluation Cybersecurity incident response requirements
🟦	Database Administrator	OM-DTA-001	2172	Administers databases and/or data management systems that allow for the secure storage, query, protection, and utilization of data.	System and data security Data systems threats and vulnerabilities Disaster Recovery Planning Data back-up and recovery Identity, credentials and authentication
🟦	Data Analyst	OM-DTA-002	2172	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.	System and data security Data systems threats and vulnerabilities Disaster Recovery Planning Data back-up and recovery Identity, credentials and authentication

Activity Area/Work Category	Common Title or Work Role	NICE ID	NOC	Major Cybersecurity Responsibility (NICE and other sources)	Key Cybersecurity Competencies
	Information Manager (NICE Knowledge Manager)	OM-KMG-001	0213, 1523	Responsible for the management and administration of processes and tools that enable the organization to identify, document, and access intellectual capital and information content.	Cybersecurity risk management Business and threat context Information/data categorization System and data security Data systems threats and vulnerabilities Disaster Recovery Planning Data back-up and recovery Identity, credentials and authentication
	Technical Support Specialist	OM-STS-001	2281, 2282	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).	Business and threat context System and data security Data back-up and recovery Cyber threats and vulnerabilities Incident response Cyber systems policies, practices and operations.
	Network Operations Specialist	OM-NET-001	2281, 2282	Plans, implements, and operates network services/systems, to include hardware and virtual environments.	Business and threat context System and data security Data back-up and recovery Cyber threats and vulnerabilities Incident response Cyber systems policies, practices and operations.
	System Administrator	OM-ADM-001	2281	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	Business and threat context System and data security Data back-up and recovery Cyber threats and vulnerabilities Incident response Cyber systems policies, practices and operations. Identity, credentials and authentication

Activity Area/Work Category	Common Title or Work Role	NICE ID	NOC	Major Cybersecurity Responsibility (NICE and other sources)	Key Cybersecurity Competencies
				adhering to organizational security policies and procedures).	
	Data Systems Analyst	None	2172	Identifies, develops and analyzes data system needs for the organization. Supports, and designs and implements data systems.	Cybersecurity risk management Business and threat context System and data security Data systems threats and vulnerabilities Disaster Recovery Planning Data back-up and recovery Identity, credentials and authentication Cybersecurity tools, techniques and procedures used to protect data and data systems Encryption and PKI
	Systems Manager (Includes system, software and data systems manager roles)	None	0213	Plans, organizes, directs, controls and evaluates the activities of organizations that analyze, design, develop, implement, operate and administer computer and telecommunications software, networks and information systems	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)