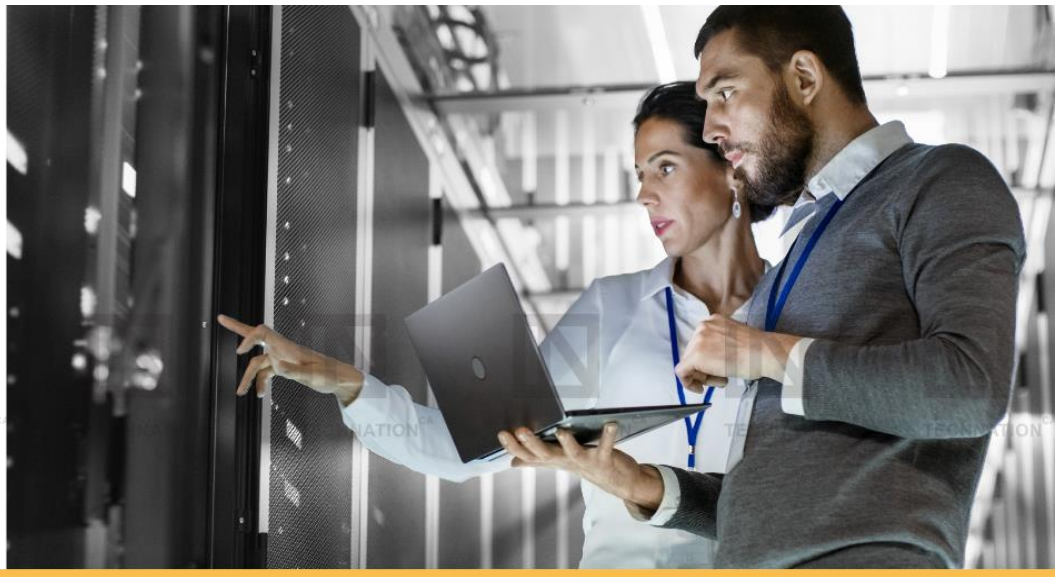

CYBERSECURITY WORKFORCE

NATIONAL OCCUPATION STANDARD

A workforce to secure Canada's digital future

APRIL 2020

TECHNATION[CA]

About TECHNATION

As Canada's national information and communications technology (ICT) business association, TECHNATION champions the development of a robust and sustainable digital economy in Canada. A vital connection between business and government, we provide our members with the advocacy, networking and professional development services that help them to thrive nationally and compete globally.

A prominent advocate for the expansion of Canada's innovative capacity, TECHNATION encourages technology adoption to capitalize on productivity and performance opportunities across all sectors. A member-driven not-for-profit, TECHNATION has served as the authoritative national voice of the $184 billion ICT industry for over 60 years. More than 39,000 Canadian ICT firms create and supply goods and services that contribute to a more productive, competitive, and innovative society. The ICT sector generates over one million jobs directly and indirectly and invests $6.1 billion annually in R&D, more than any other private sector performer.

This document has been produced by TECHNATION and contents are the sole responsibility of the author.

Acknowledgements

The Cybersecurity Talent Alliance

TECHNATION would like to commend and acknowledge the members of the Cybersecurity Talent Alliance for their leadership, oversight and insights during the National Occupational Standard (NOS) development process.

Cybersecurity Industry Professionals

TECHNATION also wishes to express its sincere appreciation to the cybersecurity professionals and stakeholders who directly or indirectly contributed to this standard through the interviews, surveys, consultations and informal discussions. While too numerous to individually mention, we sincerely appreciate the interest and expertise that the engaged members of the cybersecurity community have provided throughout this project. Their insights and perspectives were essential to the outcomes. We thank them for sharing their time, knowledge, research and experiences with us. We also look forward to their future contributions in the review process to keep this NOS current and relevant.

The Canadian Centre for Cyber Security

The Canadian Centre for Cyber Security deserves special acknowledgement for their expertise and leading the way with their Cybersecurity Curriculum Guide which helped lay the framework for the cybersecurity work in Canada and work roles used in this standard. Moreover, we will work with the Cyber Centre to ensure close alignment between our guiding documents.

The U.S. National Initiative on Cybersecurity Education (NICE)

The U.S. NICE office housed within the National Institute of Standards and Technology provided TECHNATION with support and guidance throughout this process and we appreciate their extensive work on NICE Cybersecurity Workforce Framework upon which the Canadian Cybersecurity Skills Framework was based. As well, the U.S. NICE provided detailed and rigorous descriptions of the cybersecurity work categories, specialty areas and work roles which heavily influenced the contents of this document. We look forward to working more closely with the NICE office in defining and refining our understanding of this emerging domain of work and will continue to contribute to the NICE revision process.

Government of Canada

This project is funded in part by the Government of Canada's Sectoral Initiatives Program. The opinions and interpretations in this publication are those of the author and do not necessarily reflect those of the Government of Canada.

Canada

Table of Contents

Introduction

Aim

The aim of this document is to describe the national occupation standards for core cybersecurity work for the Canadian labour market.

Cybersecurity - An emerging and enduring domain of work

Cybersecurity is defined as "the protection of digital information and the infrastructure on which it resides."[1] However, despite the internet and connected computing being around for over two decades, cybersecurity remains an emerging and evolving field of work. As such, the work has not been well defined in occupational terms and cybersecurity work is often conflated with other organizational roles. Accordingly, the NOS defines primary cybersecurity work as distinct from other occupations in information technology, security, business management, or public administration. Cybersecurity is not, however, just about technical systems, it's also about people, their behaviour and how they connect and engage with those systems.

The value of effective cybersecurity and the services and products supported by the cybersecurity professional cannot be understated. Cybersecurity work is achieving visibility across the globe as a critical and enduring career within the digital economy. In Canada, for instance:

- Our reliance on information and data systems has increased exponentially over the past decade as organizations digitize their operations and move to an online presence. This requires professionals who can design, build, and implement and maintain safe, secure and reliable information systems that can support a variety of business, operational and personal needs.
- Canadian citizens have become more aware of their Privacy rights and are increasingly concerned about how their personal data is protected by organizations. This requires experts in both online security and privacy who can advise on the various national and international standards, develop policies, identify requirements and support monitoring to better protect the privacy of Canadians.
- Cybercrime is an ever-increasing threat. With technology either as a target that can be exploited or a tool that can be used to commit other criminal acts such as theft, fraud, sexual harassment and child exploitation, cybersecurity and protective services are critical to protecting Canadians. This requires expertise to support detection and response to cyber threats as well as those who will investigate and collect digital evidence that can be used in improving protections and, when required, prosecuting offenders.

[1] Public Safety Canada (2019), National Cyber Security Strategy: Canada's Vision for Security and Prosperity in the Digital Age, retrieved 3 April 2020, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx#s11

Our recent experience with the COVID-19 crisis has amplified the need for cybersecurity across all sectors. Though often doing work behind the scenes, the Canadian cybersecurity professionals helped organizations rapidly shift to secure virtualized environments, assured security on critical health information and supply chain systems, stepped up to help protect and defend other systems of value to Canada and Canadians, and supported online security and safety to millions of every day Canadians who flocked to internet-enabled systems and applications to connect with family, friends, teachers, and colleagues.

Cybersecurity is more than just about systems, it's also about people who connect with those systems. It will continue to be required across a broad range of technologies and those employed in this emerging field have significant and lasting career opportunities that can positively affect the lives of connected Canadians and support the future of the digital economy.

Scope

For this publication, cybersecurity is inclusive of IT security, information security that involves digital artifacts, and digital security. There are inherent elements of physical, personnel, project/contract security within cybersecurity and these are identified based on the role. As cybersecurity is a highly dynamic field, detail that hinges on specific technologies or techniques have been excluded.

While there are several other contributing or adjacent cybersecurity roles as noted in the U.S. National Initiative on Cybersecurity Education (NICE), this document focuses on **core** cybersecurity roles and related competencies that are situated within the broader Canadian business context where the majority of their work is tied to organizational cybersecurity objectives and outcomes. Cybersecurity specializations that are almost solely within the intelligence, national security or policing domain are identified and detailed within the NICE Framework.

As special note on Educators

The valuable role that educators play in cybersecurity is noted. However, as educators have their own NOCs (4121, 4122, 4131) and an extensive network of occupational and professional standards, there is no need to reiterate that information within this NOS. It is recognized, however, that for every role within this NOS, qualified educators are required who have relevant experience and the ability to facilitate and assess required learning to support industry demand according to recognized standards.

National Occupational Standards

What are occupation standards?

Occupational standards describe what an individual in a particular occupation must know and be able to do to be considered 'capable' in the occupation. These standards are defined in terms of competencies, including knowledge, skills and abilities (KSAs), required to the related work effectively, safely and properly. Occupational standards provide the benchmark for competent performance in the workplace as agreed to by a

representative sample of workers, employers and other stakeholders. Occupational standards may also include or be driven by other external requirements such as legal or policy compliance.

Why is there a need for national occupation standards (NOS)?

Occupational standards describe the standards of competent and safe behaviour within a specific scope of work. Occupational standards can serve various purposes. They are often used to guide:

- Attraction and recruitment strategies
- Selection and criteria for promotion or work-related transfers
- Development of education and training
- Drafting of job descriptions
- Learning and development of employees

This NOS supports a variety of functions for cybersecurity practitioners, employers, educators and other workforce development stakeholders such as government, professional associations, sector councils, employment centres, etc. (Figure 1).

In the case of cybersecurity, it serves another purpose. As discussed, cybersecurity is a relatively new and emerging field of work where various work roles have been conflated within the domain. Accordingly, the NOS defines primary cybersecurity work as distinct from other occupations in information technology, security, business management, or public administration.

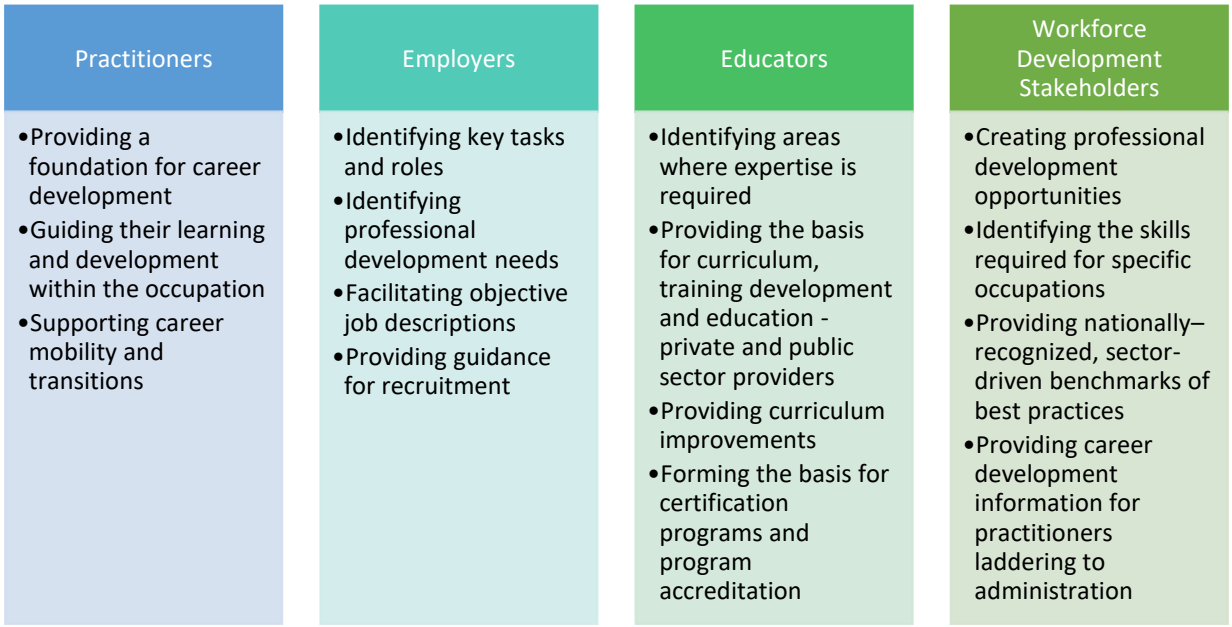

Figure 1: NOS uses

NOS Development

These national occupational standards were developed using a hybrid of industry standard methodologies leveraging recommended processes including literature review, functional and job analyses, interviews and community-centred validation processes that included practitioners, educators, employers and workforce development stakeholders.

NOS Framework and Canadian Labour Market Requirements

The United States National Institute of Standards and Technology (NIST) have developed the National Initiative on Cybersecurity Education (NICE) Cybersecurity Workforce Framework (CWF). This framework identified 7 specialty areas and 52 work roles within Cybersecurity. In conjunction with research and consultations into the Canadian cybersecurity labour market, the NICE model was refined model to focus on four key functional work areas (Figure 2). Moreover, rather than a 'cybersecurity' centric model, this model supports a business-oriented lens and situates cybersecurity within the broader organizational security context.

Exclusive of this are a very small percentage of cybersecurity specialist work roles that are defined and performed in government national security, policing or military contexts.[2] These roles are critical to the safety and security of Canadians, but tend to fall outside the general labour market and while they may receive baseline training through private and public sector training and education providers, they require significantly more training to support specific competencies, specialized tools and processes, and unique mandates. Accordingly, they are included within but not the focus of the cybersecurity skills framework. These roles and associated knowledge, skills and abilities (KSAs) are well-defined within the NICE Framework under the specialty areas of Investigate, Analyze, and Collect & Operate. A summary of these are provided in Annex B and more detail is available on the NICE website.

[2] Displayed within the medium gray shaded area in Figure 2 as Investigate, Analyze, and Collect & Operate roles.

Figure 2: Canadian Cybersecurity Skills Framework

Core Cybersecurity Roles

Recognizing that cybersecurity is a shared responsibility, this NOS describes the cybersecurity occupation in terms of work that is typically conducted full-time and requires unique knowledge, skills and abilities relative to other occupations. Moreover, as per the Canadian Cybersecurity Skills Framework discussed above, the cybersecurity occupation is further defined in terms of titles/work roles that are relevant to the Canadian labour market and broader business community within four major cybersecurity activity areas or work categories: Oversee & Govern, Design & Develop, Operate & Maintain, and Protect & Defend. These activity areas/work categories and the inherent work roles are further defined in Annex A.

Cybersecurity Adjacent Roles

There are also numerous roles associated with other organizational functions that typically contribute to organizational cybersecurity outcomes on a part-time or adhoc basis.[3] These are cybersecurity **adjacent** roles where some cybersecurity knowledge, skills and abilities are required, but they are not typically considered cybersecurity specialists.[4] For example, in most organizations, a business or policy analyst will likely be employed on a broad range of issues, only some of which will be in support of organizational cybersecurity. This is not to detract from their role in supporting

[3] This is exclusive of 'users' who have ongoing cybersecurity responsibilities regardless of organizational role.

[4] There are some professions/roles where they may be employed full-time within cybersecurity and are considered specialists, such as those employed in cyber-related law, privacy or ethics. As they are already part of another occupation and are not often part of an organization's workforce, they are not represented in this NOS. They are, however, represented in the NICE framework.

organizational cybersecurity, but only to suggest that their work involves often much more than strictly cybersecurity.

Similarly, executives, program managers, policy analysts, financial analysts, communications specialist, enterprise architects, IT technicians, etc. may have cybersecurity responsibilities but do not have full time cybersecurity functions, and are not considered core cybersecurity roles for this NOS. These roles are identified in Annex C. For example, a sampling of typical cybersecurity adjacent work roles is provided in Table 1 below. While they have cybersecurity responsibilities and require specific cybersecurity knowledge, skills and abilities, their primary responsibilities are often either broader or focused on other activities that are not directed towards cybersecurity.

Oversee & Govern	Design & Develop	Operate & Maintain
Chief Information or Technical Officer	Enterprise Architect	Systems Manager
Corporate Security Officer	System Requirements Planner	Systems Administrator
Program Manager	Business Analyst	Systems Analyst
IT Project Manager	Software Developer / Programmer	Database Administrator
Financial Analysts	Control Systems Analyst	Data Systems Analyst
Learning and Development Specialist (e.g. Security Awareness & Training)	Web Developer	Technical Support Specialist

Table 1: Sampling of typical cybersecurity adjacent work roles

Note that the Protect & Defend category is not included in the above table as that activity area/work category is exclusively employed in cybersecurity.

Review and Revision

As the cybersecurity field is very dynamic, this NOS will be reviewed annually by the Cybersecurity Talent Alliance (CTA) and workforce development stakeholders. As changes to the NOS are introduced any substantive changes will be published within a year of the review. Accordingly, all proposed changes to this NOS should be directed to the info_CTA@technationcanada.ca.

Use and Layout

Figure 3 presents the layout of each of the NOS contained within this document. Rather, as it pertains to knowledge, skills or abilities, general statements have been provided that must be interpreted by the reader within their current context.

While the majority of NOS are defined by a specific function, the trend is to go beyond specific knowledge and skill lists to competencies, which also include abilities and other characteristics that underlie effective performance. For example, for a Security Practitioner, there are certain abilities such as critical thinking, judgement and integrity which are not captured in traditional knowledge and skill-based job or task analyses. Accordingly, this NOS is competency-based and includes the information as outlined in Figure 3. Note that due to relatively recent adoption of cybersecurity as a field of work, additional information has been provided within each standard which will benefit potential users including risk-based assessment related to the role, common development pathways, and future trends that will affect key competencies.

Occupational Title

NICE Framework Reference	NICE work role title, work category and work role ID	
Functional Description & Scope	Brief description of the occupation covered	
Consequence of error or risk	Identification of key risks	
Common development pathway	Description of previous work roles/experience and potential roles beyond current occupation	
Other titles	Other job titles	
Related NOCs	Related national occupation classification code(s) and title(s).	
Major tasks	This section defines common tasks associated with the occupation. Large or complex tasks may be further broken down into sub-tasks. Tasks are distinct, observable, and measurable activities that have a beginning and an end.	
Required qualifications	Education	Post-secondary educational requirements.
	Training	Formal training and certification requirements.
	Work experience	General experience to support learning and preparation for occupational tasks.
Tools & technology	Common organizational tools and technologies which support occupational performance.	
Key competencies	Knowledge, skills, abilities and other characteristics that underlie effective performance in the occupation. For ease of use the competencies are grouped and key KSAs are provided at either a basic or advanced level of application.	
Future trends affecting key competencies	Foresight driven assessment of the implication of process, people or technological trends that will have an impact on the future occupational requirements.	

Figure 3: NOS Layout and section definitions

A note on Small and Medium Organizations (SMOs)

While there are some SMOs[5] that have employees, who may be dedicated to cybersecurity full-time, the majority do not. Cybersecurity expertise and services are often outsourced while others may assign cybersecurity responsibilities to individuals within their organization. In either case, there is increasing reliance on those identified in cybersecurity *adjacent roles* to ensure that the organizational cybersecurity needs are met. For example, this could be a CIO, IT Manager, or a Business Analyst who, in absence of a cybersecurity specialist, have increased responsibility for ensuring

[5] This includes small and medium enterprises (SMEs) and small and medium businesses (SMBs) as well as other types of non-commercial organizations.

effective cybersecurity within their organization. Described as a 'Cybersecurity Generalist', a more detailed account of these cybersecurity responsibilities and key competencies is provided in Annex D.

As each business is unique, they should carefully consider where the primary responsibilities lie and identify the information, networks and learning opportunities that support those who have cybersecurity responsibilities. Where employees such as IT or Business Analysts assume direct cybersecurity design, development or operations responsibilities, this NOS, and the extended information on cybersecurity work roles within the NICE Framework, can be used as a guide to better understand what competencies may be required for the organizational situation and context.

Cybersecurity National Occupational Standards

As defined in the NOC[6], an occupation is defined as a set of jobs that are sufficiently similar in work performed. The occupation as previously scoped includes core cybersecurity roles. For the purposes of this document, the occupation is therefore cybersecurity, and it is comprised of core cybersecurity work roles as defined in this NOS. The occupation and these roles are distinct within the Canadian national occupational framework and are 'in demand' across the Canadian labour market. All occupations are also employed within the public and private sector. Note that this includes cybersecurity and infrastructure activities that occur within security, intelligence, military, and policing environments. This does not include, however, operational policy, operational analysis, or design/development capabilities, which are largely internally prescribed and addressed within those organizations.

Relevance to National Occupation Classification (NOC) - As related to the NOC system, the majority of work roles within cybersecurity fall within skill levels A or B requiring university or college education, though there may be some roles that may be supported by skill level C requiring high school education with occupationally specific training. Cybersecurity is a field of work that is influenced by, and has an impact in, all *skill types*[7], but largely fit within the technical domain and are associated with *skill type 2* - Natural and applied sciences and closely related to computer and information systems professionals and technical occupations in computer and information systems.

As discussed, the model used for defining cybersecurity work within the Canadian labour market is based on the NICE Framework. Accordingly, the NICE information has been provided with the applicable NOS, where available, for both **core** (Annex A) and **adjacent** roles (Annex C). Note that as the focus is on core cybersecurity roles within the occupation, the NOS descriptors are detailed. However, there are many cybersecurity adjacent roles within national and organizational security contexts. As

[6] Canada (2020), National Occupational Classification FAQ, retrieved 19 March 2020 from https://noc.esdc.gc.ca/Home/FrequAskedQuestions/84ecba341f774ecc97931fcf09713b80
[7] NOC Skill Type identifies the industry of the occupation

each of the adjacent roles already stem from an existing profession and may have an occupational standard, only cybersecurity relevant competencies have been included.

Annex A - Core Cybersecurity Roles

The core cybersecurity roles are divided into major work categories/occupational sub-groups similar to those established in the NICE[8]:

- **Oversee & Govern -** Overarching responsibility for this occupational sub-group is leadership and management of the cybersecurity program. This includes technical and non-technical roles.
- **Design & Develop (Securely Provision in the NICE) -** This occupational sub-group supports design and development of the digital infrastructure, systems and software. This includes largely technical roles.
- **Operate & Maintain -** The primary responsibility of this occupational sub-group is ensuring secure operations of the digital systems and data management. All roles within this sub-group are technical roles.
- **Protect & Defend -** This occupational sub-group is focused on cybersecurity operations. All roles within this occupational sub-group are technical roles.

Common competencies (cybersecurity professional foundations)

For all of the core cybersecurity roles regardless of activity area/work category, there are a number of common competencies that are applied at the basic, intermediate, or advanced level depending on the role. All cybersecurity professionals, regardless of role, should have a **basic ability to apply** the following in their work domain/context:

- IT systems and networking
- Systems architecture and models
- Internet protocols, systems and devices
- Cybersecurity foundations
    - Integrated security framework
    - Cybersecurity strategies and approaches
    - Threat landscape and common threat surfaces (personnel, physical, IT/logical, supply chain)
    - Cyber threat intelligence process and sources
    - Cybersecurity analytics
    - Cybersecurity management policies, processes and best practices
    - Cybersecurity systems, tools and applications
    - Legislation and compliance (e.g. privacy, information sharing, reporting, mandatory standards, etc.)
    - National and industry standards
- Problem-solving and complex thinking in dynamic environments
- Maintaining broader security situational awareness
- Self-awareness regarding knowledge, skills and abilities required to respond to business, threat and technical changes.

[8] Of note, the work categories of Investigate, Analyze and Collect and Operate are only summarized within this document as they are fully defined within the NICE framework and typically fall within the responsibility of military and policing occupations.

- Continuous learning to support currency in knowledge of emerging threats, technological innovations in security, and the changing cybersecurity landscape.
- Communications (oral and verbal) suited to organizational context including drafting and writing technical reports
- Strategic thinking and business acumen to include understanding the business and risk context for cybersecurity
- Teamwork/collaborating with others including non-cybersecurity professionals
- Ethics and professional responsibilities
- Cybersecurity training and awareness within their domain

Oversee & Govern

Overarching responsibility for this activity area/work category is leadership and management of the cybersecurity program for the organization. The majority of the work within this occupational sub-group is conducted by those within recognized occupational skill groups such as management (senior managers, middle managers) and business, finance and administrative occupations (e.g. business analysts, finance analysts, risk analysts, communications). Consequently, many of the relevant work roles within this category are adjacent (non-core) roles that include policy, communications, training and awareness, that are defined in Annex C. The core work roles within this activity area/work category are:

- Chief Information Security Officer (CISO)
- Information Systems Security Officer
- Information Security Auditor

For the Oversee & Govern activity area/work category, they will typically require advanced capabilities that relate to organizational planning, measurement and management of cybersecurity.

Chief Information Security Officer (CISO)

NICE Framework Reference	Oversee and Govern, OV-EXL-001, Executive Cyber Leadership
Functional Description	An executive level role with accountability and responsibility for digital/information security activities of the organization. This includes planning, overseeing and managing strategy development and implementation, cybersecurity operations, as well as budget and resources that ensure protection of the enterprise information assets throughout the supply chain. Employed throughout the public and private sectors.
Consequence of error or risk	Error, neglect, outdated information or poor judgment could result in organizational decisions that can have a significant impact on the business. Lack of a full appreciation of the business needs for security will jeopardize the security posture of the organization in the face of evolving threats.
Development pathway	This is often considered the pinnacle of a cybersecurity career within a given organization. A CISO often has extensive experience (10+ years) in IT or systems, preferably with cybersecurity management experience. As an executive level position, the pathway also includes competency development including training, education and experience outside of the technical field.
Other titles	▪ Chief Security Officer ▪ Departmental Security Officer ▪ Information Security Director Note: depending on the size of the organization and the reliance on information technology, this occupational role may be subsumed within the responsibilities of the Chief Information Officer, Chief Technology Officer, Chief Resiliency Officer or similar role.
Related NOCs	0012 - Senior government managers and officials 0013 - Senior managers - financial, communications and other business services
Tasks	▪ Collaborate with key stakeholders to plan and establish an effective cybersecurity risk management program. ▪ Ensure compliance with the changing laws and applicable regulations ▪ Develop and implement strategic plans that are aligned to the organizational objectives and security requirements ▪ Direct and approve the design of cybersecurity systems ▪ Identify, acquire and oversee management of financial, technical and personnel resources required to support cybersecurity objectives ▪ Advise other senior management on cybersecurity programs, policies, processes, systems, and elements ▪ Ensure development and implementation of security controls to support organizational objectives ▪ Review, approve, oversee monitoring of cybersecurity policies and controls ▪ Ensure incident response, disaster recovery and business continuity plans are in place and tested

<table>
<tr><td></td><td colspan="2">▪ Draft terms of reference, oversee and review cybersecurity investigations
▪ Maintain a current understanding the IT threat landscape for the business context;
▪ Schedule and oversee security assessments and audits
▪ Oversee and manage vendor relations related to acquired IT security products and services
▪ Provide training and mentoring to security team members
▪ Supervise or manage protective or corrective measures when a cybersecurity incident or vulnerability is discovered.</td></tr>
<tr><td rowspan="3">Required qualifications</td><td>Education</td><td>Bachelor’s degree in computer science or related discipline or equivalent training and experience.</td></tr>
<tr><td>Training</td><td>Role-based training to support senior level management of security preferred.</td></tr>
<tr><td>Work experience</td><td>Significant (5-10 years) experience in IT domain with 3-5 years’ experience in cybersecurity management roles.</td></tr>
<tr><td>Tools & Technology</td><td colspan="2">▪ Strategic and business plans
▪ Threat and risk assessments
▪ Vulnerability management processes and vulnerability assessments
▪ Incident management processes and procedures
▪ Security event and incident management systems and/or incident reporting systems and networks,
▪ Cybersecurity risk management processes & policies
▪ Privacy and security legislation
▪ Organizational security infrastructure and reporting systems</td></tr>
<tr><td>Competencies</td><td colspan="2">Underpinning this occupation are those competencies demonstrated for an executive level which include those identified within the NICE framework.

Basic application of the following KSAs:
☐ Integrated/organizational security concepts, principles and practice (software, system, data, physical and personnel)
☐ Preventative technical, operational and management controls available and organizational responsibilities for those controls
☐ Sector/context relevant threats, business needs and technical infrastructure
☐ Project management and security requirements throughout the project lifecycle
☐ Supply chain vulnerabilities and integrity

Advanced application of the following KSAs:
☐ Organizational threats and vulnerabilities including:
☐ Cybersecurity threat landscape
☐ Vulnerability management requirements and the range of potential mitigations available when a vulnerability management protocol does not exist
☐ Organizational security infrastructure including protective and defensive systems
☐ Developing, implementing and allocating resources, personnel and technology to address organizational security objectives.
☐ Identifying requirements and developing cybersecurity and cybersecurity risk management policies and procedures.</td></tr>
</table>

	☐ Supplier management (if IT or security services are outsourced) ☐ Organizational communications, public communications and communicating during a crisis. ☐ Cybersecurity program management, measures and monitoring
Future Trends Affecting Key Competencies	▪ The increased reliance on virtualized and/or 'cloud-based' services will require knowledge of responsibilities of the services provider including their cybersecurity responsibilities relative to organizational cybersecurity risks. As the primary security advisor to senior management, this discussion will be led by the CISO, therefore a full appreciation of the business risks is required. ▪ If practiced within the organization, there will be a requirement to fully understand the security implications of 'bring your own devices' (BYOD) and managing the associated risks. ▪ Increased use of automated tools, aided by artificial intelligence, will require understanding of how the tools will be integrated into the organizational security infrastructure and the implications to personnel, resources, procedures, and policies. This will need to be integrated into a security strategy and action plan for the organization. ▪ Increased use of automated tools by threat actors poses challenges for organizations that do not have complementary defensive tools. Accordingly, creative, locally relevant mitigation strategies will be required. ▪ Mechanisms to support the required level of trust and organizational risk will need to be in place to support monitoring and reporting of results from automated tools. Consequently, there will be a need to understand organizational risks posed, measures of security and what policies, processes, or procedures need to be in place. Actions will also need to consider the organizational constraints and alternatives. ▪ The emergence and use of quantum technologies by threat actors will fundamentally change encryption security. This will require advanced knowledge and skills related to implementing a quantum safe strategy and supporting processes within the organization.

Information System Security Officer (ISSO)

NICE Framework Reference	None.
Functional Description	This is an adhoc management role within cybersecurity that is primarily engaged in oversight and reporting of information system security within a department, branch, or organization. This role is primarily responsible for local planning and management of the security of system(s) over which they have been given authority. This role may report indirectly or directly to the CISO or another authority (e.g. Corporate Security Officer or Chief Information Officer or their delegate).
Consequence of error or risk	Error, neglect, outdated information or poor judgment could result in decisions or actions that could compromise the security of the system over which the ISSO has authority. Depending on the system, this could have a significant impact on the business. A lack of a full appreciation of the business needs for security will jeopardize the security posture of the organization in the face of evolving threats.
Development pathway	This is commonly a part-time role assigned or assumed by an individual with some technical experience but is not normally a 'cybersecurity professional'. In small and medium organizations this role may also be an IT manager or senior manager with some technical or security experience.
Other titles	▪ Chief Security Officer ▪ Departmental Security Officer ▪ Information Security Director Note: depending on the size of the organization and the reliance on information technology, this occupational role may be subsumed within the responsibilities of the Chief Information Officer, Chief Technology Officer, Chief Resiliency Officer or similar role.
Related NOCs	0213 – Communication and Information Systems Managers
Tasks	▪ Collaborate with key stakeholders to plan and establish an effective cybersecurity risk management program. ▪ Ensure compliance with the changing laws and applicable regulations ▪ Develop and implement strategic plans that are aligned to the organizational objectives and security requirements ▪ Direct and approve the design of cybersecurity systems ▪ Identify, acquire and oversee management of financial, technical and personnel resources required to support cybersecurity objectives ▪ Advise other senior management on cybersecurity programs, policies, processes, systems, and elements ▪ Ensure development and implementation of security controls to support organizational objectives ▪ Review, approve, oversee monitoring of cybersecurity policies and controls ▪ Ensure incident response, disaster recovery and business continuity plans are in place and tested ▪ Draft terms of reference, oversee and review cybersecurity investigations

<table>
<tr><td></td><td colspan="2">Maintain a current understanding the IT threat landscape for the business context;
Schedule and oversee security assessments and audits
Oversee and manage vendor relations related to acquired IT security products and services
Supervise or manage protective or corrective measures when a cybersecurity incident or vulnerability is discovered.</td></tr>
<tr><td rowspan="3">Required qualifications</td><td>Education</td><td>Post-secondary education in a cyber or IT related field (e.g.; Computer engineering, Computer Science, Information Technology, Business Technology Management – Digital Security or equivalent)</td></tr>
<tr><td>Training</td><td>As required to support the role for example cybersecurity team management, incident management and cybersecurity planning would be an asset.</td></tr>
<tr><td>Work experience</td><td>3-5 years’ experience in IT domain with some management experience.</td></tr>
<tr><td>Tools & Technology</td><td colspan="2">Strategic and business plans
Threat and risk assessments
Vulnerability management processes and vulnerability assessments
Incident management processes and procedures
Security event and incident management systems and/or incident reporting systems and networks,
Cybersecurity risk management processes & policies
Privacy and security legislation
Organizational security infrastructure and reporting systems</td></tr>
<tr><td>Competencies</td><td colspan="2">Underpinning this occupation are those competencies demonstrated for an executive level which include those identified within the NICE framework.

Basic application of the following KSAs:
☐ Integrated/organizational security concepts, principles and practice (software, system, data, physical and personnel)
☐ Preventative technical, operational and management controls available and organizational responsibilities for those controls
☐ Sector/context relevant threats, business needs and technical infrastructure
☐ Project management and security requirements throughout the project lifecycle
☐ Supply chain vulnerabilities and integrity

Advanced application of the following KSAs:
☐ Organizational threats and vulnerabilities including:
o Cybersecurity threat landscape
o Vulnerability management requirements and the range of potential mitigations available when a vulnerability management protocol does not exist
o Organizational security infrastructure including protective and defensive systems
☐ Cybersecurity team management
☐ Developing, implementing and allocating resources, personnel and technology to address organizational security objectives.</td></tr>
</table>

	☐ Identifying requirements and developing cybersecurity and cybersecurity risk management policies and procedures. ☐ Supplier management (if IT or security services are outsourced) ☐ Organizational communications, public communications and communicating during a crisis. ☐ Cybersecurity program management, measures and monitoring
Future Trends Affecting Key Competencies	▪ The increased reliance on virtualized and/or 'cloud-based' services will require knowledge of responsibilities of the services provider including their cybersecurity responsibilities relative to organizational cybersecurity risks. As a senior security advisor to management, this role will need a full appreciation of the business risks is required. ▪ If practiced within the organization, there will be a requirement to fully understand the security implications of 'bring your own devices' (BYOD) and managing the associated risks. ▪ Increased use of automated tools, aided by artificial intelligence, will require understanding of how the tools will be integrated into the organizational security infrastructure and the implications to personnel, resources, procedures, and policies. This will need to be integrated into a security strategy and action plan for the organization. ▪ Increased use of automated tools by threat actors poses challenges for organizations that do not have complementary defensive tools. Accordingly, creative, locally relevant mitigation strategies will be required. ▪ Mechanisms to support the required level of trust and organizational risk will need to be in place to support monitoring and reporting of results from automated tools. Consequently, there will be a need to understand organizational risks posed, measures of security and what policies, processes, or procedures need to be in place. Actions will also need to consider the organizational constraints and alternatives. ▪ The emergence and use of quantum technologies by threat actors will fundamentally change encryption security. This will require advanced knowledge and skills related to implementing a quantum safe strategy and supporting processes within the organization.

Information Security (IS) Auditor

NICE Framework Reference	None. Associated with OV-PMA-005 IT Program Auditor	
Functional Description	A specialized auditor role, an information security auditor is responsible for evaluating and reporting on the security and effectiveness of IT systems and related controls in support of organizational information / data security, IT systems and their components. The audit conducted is often reported to a senior manager with recommendations for changes or improvements.	
Consequence of error or risk	Error, neglect, outdated information or poor judgment could result in an incomplete or inaccurate audit that does not identify critical system or process issues and fails to address organizational security requirements and increasing the potential risks of a compromise or security system failure.	
Development pathway	Employment in this role is often preceded by formal education with a degree or diploma in an IT field as well as experience in an organizational cybersecurity role. There is also a requirement for specialized training and education in information system and information security audit practices.	
Other titles	Cybersecurity auditor Security control assessor IT security auditor	
Related NOCs	2171 - Information systems analysts and consultants 2147 – Computer Engineers	
Tasks	▪ Collaborate with key stakeholders to establish an effective information security audit strategy which defines both internal and external audit requirements ▪ Liaise with external auditors as required to support organizational requirements ▪ Ensure compliance with the changing laws and applicable regulations ▪ Develop and implement detailed internal audit plans that are aligned to the organizational objectives and security requirements ▪ Identify, acquire and oversee management of financial, technical and personnel resources required to support IS audit activities ▪ Develop and deploy policy testing on IS systems ▪ Review security assessment and authorization activities ▪ Advise other senior management on cybersecurity programs, policies, processes, systems, and elements ▪ Review and interpret cybersecurity / information security policies and controls ▪ Maintain a current understanding the IT threat landscape for the business context ▪ Schedule and conduct internal IS audits ▪ Analyze and interpret and external IS audit results ▪ Report results and provide recommendations to leadership and system owner(s).	
Required qualifications	Education	Post-secondary education in a cyber or IT related field (e.g.; Computer engineering, Computer Science, Information Technology, Business

		Technology Management – Digital Security or equivalent)
	Training	Specialized training in IT or information system audit and security audit.
	Work experience	Experience (3-5 years) in cybersecurity with preference in systems analytics (e.g. cybersecurity operations analyst, vulnerability analyst, IT systems security analyst)
Tools & Technology	▪ Strategic and business plans ▪ Threat and risk assessments ▪ Vulnerability management processes and vulnerability assessments ▪ Incident management processes and procedures ▪ Cybersecurity risk management processes & policies ▪ Compliance requirements including privacy and security legislation ▪ Organizational security infrastructure and reporting systems ▪ IS audit tools and systems ▪ Vulnerability assessments ▪ Penetration testing results ▪ IT systems performance measures	
Competencies	Basic application of the following KSAs: ☐ Project and program management ☐ IT audit policies, practices and procedures Advanced application of the following KSAs: ☐ Legal, policy and compliance requirements ☐ Business objectives and how IT/data/systems enable the business ☐ Information security audit polices, practices and procedures ☐ Integrated/organizational security concepts, principles and practice (software, system, data, physical and personnel) ☐ External audit resources, competencies and capabilities ☐ Sector/context relevant threats, business needs and technical infrastructure ☐ Organizational security responsibilities, accountabilities and performance measures ☐ Cybersecurity program management, measures and monitoring ☐ Organizational cybersecurity controls and responsible agents ☐ Organizational threats and vulnerabilities including: o Cybersecurity threat landscape o Vulnerability assessments and application of mitigations o Organizational security infrastructure including protective and defensive systems ☐ Security throughout the system / software development lifecycle ☐ Supply chain security ☐ System integration, testing and deployment ☐ Supplier management (if IT or security services are outsourced) and supply arrangements	
Future Trends Affecting Key Competencies	▪ The increased reliance on virtualized and/or ‘cloud-based’ services will require knowledge of responsibilities of the services provider and linkages with organizational systems. ▪ If practiced within the organization, there will be a requirement to fully understand the security implications of ‘bring your own devices’ (BYOD) and managing the associated risks.	

	▪ Increased use of automated tools, aided by artificial intelligence, will require understanding of how the tools are integrated into the organizational security infrastructure, the implications to security controls and how they will be measured and assessed against security goals. ▪ Increased use of automated tools by threat actors pose challenges for organizations that do not have complementary defensive tools. Therefore, audits of defensive tools and systems will evolve. ▪ Mechanisms to support the required level of trust and organizational risk will need to be in place to support monitoring and reporting of results from automated tools. Consequently, there will be a need to understand how those tools operate, how their performance can be measured and what audit activities may be necessary. ▪ The emergence and use of quantum technologies by threat actors will fundamentally change encryption security. This will require knowledge and skills related to implementing a quantum safe strategy within the organization.

Design & Develop

This activity area/work category is involved with developing secure infrastructure, systems and software. This is a highly technical branch of cybersecurity work. The majority of this work falls within the responsibilities of computer engineers (2147), computer programmers and interactive media developers (2174), information systems testing technicians (2283), and information systems analysts and consultants (2171). As these are common occupations, which are also defined within the NICE, they have not been included within this document.

The following occupations are addressed within this NOS:

- Security Architect
- Security Engineer/Security Engineering Technologist
- Secure Software Assessor
- Security Testing and Evaluation Specialist
- Operational Technology Systems Analyst
- Supply Chain Security Analyst
- Information Systems Security Developer
- Security Automation Engineer/Analyst
- Cryptanalyst / Cryptographer

Given the focus of this activity area, the emphasis is on applying deep technical understanding within a business context to better support organizational cybersecurity outcomes.

Security Architect

NICE Framework Reference	Securely Provision, SP-ARC 002, Security Architect
Functional Description	Designs, develops and oversees the implementation of network and computer security structures for an organization, ensuring security requirements are adequately addressed in all aspects of the infrastructure, and the system supports an organization's processes
Consequence of error or risk	Error, neglect, outdated information or poor judgment could result in flawed designs or architectures that could fail or experience exploitable vulnerabilities which could place IT systems upon which the organization relies in jeopardy. Lack of a full appreciation of the business needs for security will jeopardize the security posture of the organization in the face of evolving threats.
Development pathway	Primarily following education and a career pathway from an existing enterprise architect role, this is an emerging specialist role primarily employed in large tech-enabled organizations, shared services or systems or security providers.
Other titles	Enterprise security architect
Related NOCs	2147 Computer engineers (except software engineers and designers) 2171 Information systems analysts and consultants
Tasks	▪ Collaborate with key stakeholders to establish an effective cybersecurity risk management program ▪ Ensure compliance with the changing laws and applicable regulations ▪ Define and review an organization's technology and information systems, and ensure security requirements ▪ Recognize appropriate disaster recovery plans and business continuity functions, including any failover or backup requirements for system restoration ▪ Plan, research, and develop robust security architectures for systems and networks ▪ Research current and emerging technologies to understand capabilities of required networks or systems ▪ Prepare cost estimates and identify integration issues ▪ Conduct vulnerability testing, risk analyses and security assessments ▪ Research and develop a system security context, and define security assurance requirements based on industry standards and cybersecurity policies and practices ▪ Ensure the acquired or developed systems and architectures are consistent with an organization's cybersecurity policies and practices ▪ Perform security reviews and identify gaps or determine the capability of security architectures and designs (e.g., firewall, virtual private networks, routers, servers, etc.), and develop a security risk management plan ▪ Prepare technical reports that document the architecture development process

<table>
<tr><td></td><td colspan="2">▪ Document and address an organization’s information security, cybersecurity architecture, and systems security engineering requirements throughout a system life cycle
▪ Advise on security requirements and risk management process activities
▪ Support incident management and post-analysis advising on recovery operations
▪ Develop, deliver, and oversee related cybersecurity training material and educational efforts related to role</td></tr>
<tr><td rowspan="3">Required qualifications</td><td>Education</td><td>Post-secondary education in IT infrastructure and architecture (e.g.; computer engineering, IT systems architecture)</td></tr>
<tr><td>Training</td><td>Specialized training in security architecture concepts, principles, and practices. Training to support security tools needed to support role.</td></tr>
<tr><td>Work experience</td><td>Previous training and experience in IT security infrastructure, requirements analysis or program management is preferred – 5-10 years of relevant IT experience for advanced-level.</td></tr>
<tr><td>Tools & Technology</td><td colspan="2">▪ Strategic and business plans
▪ Threat and risk assessments
▪ Systems architectures
▪ IT mapping tools and applications
▪ Incident management processes and procedures
▪ Security event and incident management systems and/or incident reporting systems and networks,
▪ Cybersecurity risk management processes & policies
▪ Privacy and security legislation
▪ Organizational security infrastructure and reporting systems</td></tr>
<tr><td>Competencies</td><td colspan="2">Underpinning this occupation are those competencies demonstrated for an executive level which include those identified within the NICE framework.

Advanced application of the following KSAs:
☐ Business needs for security
☐ Legal, policy and compliance requirements
☐ Integrated/organizational security concepts, principles and practice (software, system, data, physical and personnel)
☐ Preventative technical, operational and management controls available and organizational responsibilities for those controls
☐ Sector/context relevant threats, business needs and technical infrastructure
☐ Project management and security requirements throughout the project lifecycle
☐ Cryptography and cryptographic key management concepts;
☐ Virtual Private Network devices and encryption;
☐ Engineering concepts and practices as applied to systems security and systems architecture
☐ Security architecture concepts and enterprise architecture reference models;
☐ Security assessment and authorization processes
☐ Authentication, authorization, and access control methods
☐ System testing and evaluation methodologies and processes</td></tr>
</table>

	☐ Application security system concepts and functions ☐ System life cycle management principles, including software security and usability ☐ Industry standards and organizationally accepted analysis principles and methods ☐ Configuring and using software-based computer protection tools ☐ Designing hardware and software solutions ☐ Cybersecurity program management, measures and monitoring ☐ Incident management and system recovery planning and operations
Future Trends Affecting Key Competencies	▪ The increased reliance on virtualized and/or 'cloud-based' services will require deep knowledge at the intersection between organizational and service providers architectures to determine and manage cybersecurity risks. ▪ If practiced within the organization, there will be a requirement to fully understand the security implications of 'bring your own devices' (BYOD) and how security controls are integrated into the organizational infrastructure. ▪ Increased use of automated tools, aided by artificial intelligence, will require understanding of how the tools will be integrated into the overall security architecture and infrastructure and the implications to personnel, resources, procedures, and policies. ▪ Increased use of automated tools by threat actors pose challenges for organizations that do not have complementary defensive tools. Accordingly, creative, locally relevant mitigation strategies will be required that will need to be integrated into the security architecture. ▪ Mechanisms to support the required level of trust and organizational risk will need to be in place to support monitoring and reporting of results from automated tools. Consequently, there will be a need to understand organizational risks posed, measures of security and what policies, processes, or procedures need to be in place to support an integrated security architecture. ▪ The emergence and use of quantum technologies by threat actors will fundamentally change encryption security. This will require knowledge and skills related to implementing a quantum safe strategy within the organization and integrating it across the architecture.

Security Engineer[9]/Technologist

This includes:

Encryption Engineer/Technologist

Operational Technology Engineer/Technologist

NICE Framework Reference	Securely Provision, R&D Specialist, SP-TRD-001
Functional Description	Given references, organizational security documentation, IT security guidance and required tools and resources, researches and defines the business needs for security and ensures that they are addressed throughout all aspects of system engineering and throughout all phases of the System Development Lifecycle (SDLC).
Consequence of error or risk	Error, neglect, outdated information or failure to account for organizational requirements, business needs and threats could result in poor systems design and/or integration of systems/devices that create exploitable vulnerabilities which can have significant implications to organizational objectives including the potential for catastrophic systems failure.
Development pathway	Typically follows formal education and 5-10 years' experience in related IT engineering, systems design, or systems integration functions. This role often requires advanced training, education or experience related to system capabilities. May be employed in general or specialized contexts such as Cryptography / Encryption, security testing and evaluation, or Operational Technology (ICS/OCS/SCADA).
Other titles	▪ Security Designer ▪ Security Requirements Analyst ▪ Network Security Engineer ▪ Security engineering technologist ▪ Operational technology engineer ▪ Encryption engineer
Related NOCs	2133 Electrical and electronics engineers 2147 Computer engineers (except software engineers and designers) 2171 Information systems analysts and consultants 2241 Electrical and electronics engineering technologists and technicians
Tasks	▪ Define/validate business needs for security & security requirements ▪ Review and analyze security IT / OT architectures & design documents, as well as related systems, protocols, services, controls, appliances, applications, encryption and crypto algorithms relative to security requirements and industry standards ▪ Develop and review system use cases ▪ Identify the technical threats to, and vulnerabilities of, systems ▪ Manage the IT /OT security configuration

[9] **Important Note:** A security engineer is a nascent field that is normally developed from the professional engineering fields of communications and electronics engineering, IT systems engineering or similar field. In Canada, the term 'engineer' means a licensed professional engineer as described in the local jurisdiction. Accordingly, all security engineers must be licensed to practice 'engineering' within their jurisdiction. However, this NOS is intended to address specific cybersecurity occupational standards for those fulfilling a security engineer or security engineering technologist role with the understanding that pure engineering tasks are out of scope for the engineering technologist.

<table>
<tr><td></td><td colspan="2">

Analyze IT / OT security tools and techniques
Analyze the security data and provide advisories and reports
Analyze IT / OT security statistics
Prepare technical reports such as IT security solutions option analysis and implementation plans
Provide Independent Verification and Validation (IV&V) on IT / OT Security Projects
Oversee IT / OT security audits
Advise on security of IT /OT projects
Advise on IT / OT security policies, plans and practices
Review system plans, contingency plans, Business Continuity Plans (BCP) and Disaster Response Plans (DRP)
Design/development and conduct IT / OT security protocols tests and exercises
Review, develop and deliver training materials

</td></tr>
<tr><td rowspan="3">Required qualifications</td><td>Education</td><td>Relevant engineering degree or technologist diploma (depending on organizational requirements).</td></tr>
<tr><td>Training</td><td>Valid industry level certification in related cybersecurity specialization (e.g. network security, cryptography, systems integration, etc.).</td></tr>
<tr><td>Work experience</td><td>Moderate experience (3-5 years) in security and associated systems design, integration, testing and support.</td></tr>
<tr><td>Tools & Technology</td><td colspan="2">

Threat and risk assessment tools and methodologies
Protective and defensive systems including firewalls, anti-virus software and systems, intrusion detection and protection systems, scanners and alarms
Security event and incident management systems and/or incident reporting systems and networks
Authentication software and systems
Vulnerability management processes and vulnerability assessment systems including penetration testing if used
Security services provided if applicable
Security testing and evaluation tools and techniques

</td></tr>
<tr><td>Competencies</td><td colspan="2">The security engineer/engineering technologist requires a basic level of application of the following KSAs while the security engineer requires an advanced level of application of the following KSAs:

☐ Security engineering models
☐ Defining and communicating security approaches that support organizational requirements
☐ International security standards and compliance
☐ Security architecture concepts and enterprise architecture reference models
☐ SDN, NFV, and VNF functions
☐ Systems security during integration and configuration
☐ Security assessment and authorization processes
☐ Security testing and evaluation methodologies and processes
☐ Security across the system / software development lifecycle
☐ Vulnerability assessment and penetration testing methodologies and applications
☐ Systems and software testing and evaluation methodologies
☐ Evidence-based security design</td></tr>
</table>

	☐ Developing and testing threat models ☐ Project management and security assessment throughout the project lifecycle ☐ Procurement processes and supply chain integrity assessments ☐ Advising on security requirements, policies, plans and activities ☐ Drafting and providing briefings and reports to different audience levels (users, managers, executives) In addition, in High Assurance, Encryption, and Cryptographic environments: ☐ Security governance in high assurance, encryption and cryptographic environments ☐ Advanced threat modeling and risk management in sensitive information environments ☐ Key management policies and practices (including Communications Security [COMSEC]) ☐ Emissions security standards ☐ Physical and IT security zoning ☐ Cryptography and encryption including algorithms and cyphers ☐ Stenography ☐ Testing and implementing Cross-domain solutions ☐ Key management, key management products and certification lifecycle ☐ Advanced persistent and sophisticated threat actor tactics, techniques and procedures. ☐ Quantum safe/resistant technology ☐ Assessment and auditing encryption/cryptographic networks and systems In addition, within Operational Technology (ICS/OCS/SCADA) environments: ☐ Industry standards and organizationally accepted analysis principles and methods ☐ Control system: o architecture and system defenses o governance and management in various environments o attack surfaces, threats and vulnerabilities o security monitoring, tools and techniques ☐ IT systems and protocols within control systems configurations ☐ Integration of IT and OT control systems ☐ Hardening and monitoring OT control systems ☐ Security assessment and authorization process of OT systems ☐ Incident response planning and activities in control system environments ☐ Business continuity planning and disaster recovery plans and activities in a control system environment
Future Trends Affecting Key Competencies	▪ The increased reliance on virtualized and/or 'cloud-based' services will require knowledge of responsibilities of the services to be provided and how they are integrated into the organizational networks. ▪ If practiced within the organization, there will be a requirement to fully understand the implications of 'bring your own device' (BYOD) policies. This means that regardless of the device capabilities, there will need to be an assessment of the risks posed to the organization and mitigations implemented to the level of acceptable risk. ▪ Increased use of automated tools, aided by artificial intelligence, will require understanding of how the tools will be integrated into the organization and the potential security implications. If automated security tools will be used, testing, integration and monitoring requirements will

	need to be defined and those responsible for these activities will need to be advised / trained on the resulting process and procedural changes. ▪ Increased use of automated tools by threat actors pose challenges for organizations that do not have complementary defensive tools. Accordingly, creative, locally relevant mitigation strategies will be required. This will require well-honed critical and abstract thinking abilities. ▪ Mechanisms to support the required level of trust and organizational risk will need to be in place to support monitoring and reporting of results from automated tools. Consequently, there will be a need for increased understanding of organizational risks posed within the dynamic threat environment. ▪ The emergence and use of quantum technologies by threat actors will fundamentally change encryption security. This will require knowledge and skills related to implementing a quantum safe strategy within the organization.

Secure Software Assessor

NICE Framework Reference	Security Provision, SP Dev-001, Secure Software Assessor	
Functional Description	Given references, organizational security documentation, cybersecurity guidance and required tools and resources, analyzes the security of new or existing computer applications, software, or specialized utility programs and provides actionable results.	
Consequence of error or risk	Error, neglect, outdated information could result in vulnerabilities in software and web-based tools can place organizational systems and services at risk.	
Development pathway	Typically follows formal education and 5-10 years' experience in the software development field. This role often requires advanced training, education or experience related to secure software and vulnerability assessment activities for software / application security.	
Other titles	▪ Secure software developer/programmer ▪ Software testing and evaluation specialists ▪ Vulnerability analyst / assessor	
Related NOCs	2171 Information systems analysts and consultants 2173 Software engineers/designers 2174 Computer programmers and interactive media developers	
Tasks	▪ Define/validate business needs for security & security requirements ▪ Review and analyze security IT architectures & design documents, as well as related systems, protocols, services, controls, appliances, applications, encryption and crypto algorithms relative to security requirements and industry standards ▪ Research, analyze and implement secure application development processes and techniques; ▪ Analyze the security data and provide advisories and reports ▪ Develop and conduct software system or application testing and validation procedures, programming, and secure coding, and report on functionality and resiliency; ▪ Develop and review system use cases ▪ Conduct vulnerability scans and reviews on software systems or applications, and examine controls and measures required to protect software systems or applications; ▪ Prepare reports on software systems, development and applications, patches or releases that would leave systems vulnerable; ▪ Develop countermeasures against potential exploitations of vulnerabilities in systems; ▪ Perform risk analysis whenever an application or system undergoes a change; and ▪ Prepare technical reports such as IT security solutions option analysis and implementation plans ▪ Provide Independent Verification and Validation (IV&V) on software projects ▪ Advise on software security policies, plans and practices ▪ Review, develop and deliver training materials	
Required qualifications	Education	Relevant computer science degree or diploma related to programming, software design or software development

	Training	Valid industry level certification in related secure software development and software security testing
	Work experience	Moderate experience (3-5 years) in software development followed by moderate experience (3-5 years) in secure software development activities.
Tools & Technology	▪ Software development tools, processes and protocols ▪ Threat and risk assessment tools and methodologies ▪ Protective and defensive systems including firewalls, anti-virus software and systems, intrusion detection and protection systems, scanners and alarms ▪ Open source software and application security information (e.g. OWASP) ▪ Security event and incident management systems and/or incident reporting systems and networks ▪ Software security testing and evaluation tools and techniques ▪ Authentication software and systems, ▪ Vulnerability management processes and vulnerability assessment systems including penetration testing if used ▪ Common vulnerability data bases ▪ Software development social collaboration sites (e.g. GITHUB) ▪ Security services provided if applicable	
Competencies	Basic application of the following KSAs: ☐ Security architecture concepts and enterprise information security architecture model ☐ Security assessment and authorization processes ☐ Software procurement processes and supply chain integrity assessments ☐ IT security systems testing and evaluations tools, procedures and practices Advanced application of the following KSAs: ☐ Software engineering models, processes and principles ☐ Software development lifecycle and software project management ☐ Secure coding/software development operations processes, procedures, practices, tools and techniques ☐ Business needs for security including compliance requirements ☐ Data security characteristics and requirements ☐ Security controls for software development ☐ Software development standards ☐ Secure software standards ☐ Secure software testing and evaluation methodologies and processes ☐ Vulnerability assessment and penetration testing methodologies and applications ☐ Developing and testing threat models ☐ Vulnerability scanning, assessment and analysis ☐ Penetration testing activities and techniques ☐ Investigating and analyzing software vulnerabilities and breaches ☐ Establishing and managing a secure software/ web application testing environment ☐ Advising on security requirements, policies, plans and activities ☐ Drafting and providing briefings and reports to different audience levels (users, managers, executives)	
Future Trends Affecting Key Competencies	▪ The increased reliance on virtualized and/or ‘cloud-based’ services will require knowledge of responsibilities of the services to be provided, software systems and applications used and how they are integrated into the organizational networks.	

	▪ If practiced within the organization, there will be a requirement to fully understand the implications of 'bring your own device' (BYOD) policies. This means that regardless of the device capabilities, there will need to be an assessment of the risks posed to the organization and mitigations implemented to the level of acceptable risk. ▪ Increased use of automated tools, aided by artificial intelligence, will require understanding of how the tools that may support software development, testing and integration will be used as well as the potential security implications. If automated security tools in software development and assessment, responsibilities for testing, integration and monitoring requirements will need to be defined and those responsible for these activities will need to be advised / trained on the resulting process and procedural changes. ▪ Increased use of automated tools by threat actors pose challenges for organizations that do not have complementary defensive tools. Accordingly, creative, locally relevant assessments of the robustness of software / applications security and potential mitigation strategies will be required. This will require well-honed critical and abstract thinking abilities. ▪ Mechanisms to support the required level of trust and organizational risk will need to be in place to support monitoring and reporting of results from automated tools. Consequently, there will be a need for increased understanding of organizational risks posed within the dynamic threat environment. ▪ The emergence and use of quantum technologies by threat actors will fundamentally change encryption security. This will require knowledge and skills related to implementing a quantum safe strategy as it applies to the software/application environment.

Security Testing and Evaluation Specialist

NICE Framework Reference	Securely Provision, Security Testing and Evaluation, SP-TST-001	
Functional Description	Plans, prepares, and executes tests of security devices, operating systems, software and hardware to evaluate results against defined specifications, policies, and requirements, and documents results and makes recommendations that can improve information confidentiality, integrity, and availability.	
Consequence of error or risk	Error, neglect, outdated information or poor judgment could result in IT systems, software or services being integrated and deployed with vulnerabilities that increase threat exposure and organizational risk. Resulting compromises could have a significant impact on the business.	
Development pathway	Typically follows formal education and 5-10 years' experience in IT security. This role often requires specialized training, education or experience related to systems testing and measurement.	
Other titles	Systems security assessor	
Related NOCs	2171 Information systems analysts and consultants 2147 Computer engineers (except software engineers and designers)	
Tasks	▪ Tests, evaluates, and verifies systems under development; systems exchanging electronic information with other systems; related operating system software and hardware; and security controls and devices used within an organization to determine level of compliance with defined specifications, policies, and requirements ▪ Analyze test results of operating systems, software, and hardware and make recommendations based on finding ▪ Develop test plans to address specifications, policies, and requirements ▪ Validate specifications, policies and requirements for testability ▪ Create verifiable evidence of security measure ▪ Prepare assessments that document the test results and any security vulnerabilities present ▪ Deploy, validate, and verify network infrastructure device operation ▪ Develop, deliver, and oversee training material and educational efforts ▪ Provide training and mentoring to security team members	
Required qualifications	Education	Bachelor's degree in computer science or related discipline or equivalent training and experience.
	Training	Training in system security measurement, assessment and testing.
	Work experience	Significant (5-10 years) experience in IT domain with 3-5 years' experience in systems security role supporting security assessments and IT audits preferred. Experience working in secured testing environments.
Tools & Technology	▪ Strategic and business plans ▪ Threat and risk assessments ▪ Vulnerability management processes and vulnerability assessments ▪ Incident management processes and procedures	

	▪ Security event and incident management systems and/or incident reporting systems and networks, ▪ System architecture ▪ Cybersecurity risk management processes & policies ▪ Privacy and security legislation ▪ Organizational security infrastructure and reporting systems ▪ System testing and evaluation policies tools, techniques, procedures and protocols ▪ Legislation and compliance requirements
Competencies	Basic application of the following KSAs: ☐ Security procurement processes and supply chain integrity assessments ☐ Systems engineering process Advanced application of the following KSAs: ☐ Security assessment and authorization processes ☐ IT systems testing and evaluation strategies ☐ IT systems testing and evaluation infrastructure and resources ☐ IT security systems testing and evaluations tools, procedures and practices ☐ Technical knowledge of networks, computer components, power supply technology, system protocols, cybersecurity-enabled software ☐ Network security architecture and models ☐ Conducting independent validation and verification security testing ☐ Systems testing and evaluation methods and techniques ☐ Test design, scenario development, and readiness review ☐ Systems integration testing ☐ Security assessment and authorization processes ☐ Security architecture concepts and enterprise information security architecture model ☐ Identifying test and evaluation policies and requirements ☐ Collect, analyze, verify and validate test data and translate data and test results into conclusion ☐ Designing and document test and evaluation strategies ☐ Writing technical and test and evaluation reports.
Future Trends Affecting Key Competencies	▪ The increased reliance on virtualized and/or ‘cloud-based’ services will require knowledge of responsibilities of the services provider including their cybersecurity responsibilities relative to organizational systems, how those systems are integrated and how they can be tested and evaluated. ▪ If practiced within the organization, there will be a requirement to fully understand the security implications of ‘bring your own devices’ (BYOD) and managing the associated risks to organizational systems. ▪ Increased use of automated tools, aided by artificial intelligence, will require understanding of how the tools will be integrated into the organizational security infrastructure and the implications to testing and evaluation practices. ▪ Increased use of automated tools by threat actors pose challenges that will require continuous assessment of testing and evaluation practices and required tools. ▪ Mechanisms to support the required level of trust and organizational risk will need to be in place to support monitoring and reporting of

	results from automated tools. Consequently, there will be a need to understand organizational risks posed, measures of security and what policies, processes, or procedures need to be in place and any implications on security testing and evaluation. ▪ The emergence and use of quantum technologies by threat actors will fundamentally change encryption security. This will require knowledge and skills related to implementing a quantum safe strategy relevant to testing and evaluating encryption and degree of quantum resistance.

Operational Technology Systems Analyst

NICE Framework Reference	None.
Functional Description	Responsible for providing advice and ensuring effective cybersecurity within operations technology (OT) contexts (ICS/OCS/SCADA). Works in concert with systems engineers/technologists from different disciplines that are associated to the systems that are managed through OT (e.g. fluid, power, mechanical systems engineers).
Consequence of error or risk	Error, neglect, outdated information or poor judgment could result in catastrophic failure of OT and related systems that they are used for management. In many cases, this can have a significant impact on the organizational operations and in some cases can directly result in significant human harm (e.g. in critical infrastructure systems).
Development pathway	Following technical education, often employed in IT or OT systems activities which provide the foundation for more specialized cybersecurity work in the OT environment. Similarly, cybersecurity professionals that normally work in an IT environment, may cross over to OT systems with the benefit of specialized training and education in OT and systems integration.
Other titles	OT security advisor OT security technician Security Analyst - ICS/OCS/SCADA
Related NOCs	2133 Electrical and electronics engineers 2147 Computer engineers (except software engineers and designers) 2171 Information systems analysts and consultants 2241 Electrical and electronics engineering technologists and technicians
Tasks	▪ Collaborate with key stakeholders to establish an effective cybersecurity risk management program across the OT environment. ▪ Research and support design of cybersecurity solutions within OT context ▪ Ensure compliance with the changing laws and applicable regulations ▪ Draft, implement, and maintain IT/OT security policies, standards, and procedures. ▪ Monitor and manage cybersecurity requirements and controls across the OT environment ▪ Assess and analyze cybersecurity posture across OT systems and recommend remediation/risk management for vulnerabilities. ▪ Working with other stakeholders, support design and development of security solutions to enable business and technical requirements within the OT environment ▪ Manage the technical integration between IT and OT ▪ Define and maintain tool sets and procedures that support monitoring and management of OT ▪ In concert with other stakeholders, develop cybersecurity incident response plans clearly defining the role of those engaged in management and maintenance of OT systems ▪ Prepare technical reports

<table>
<tr><td></td><td colspan="2">▪ Develop, deliver, and oversee related cybersecurity training material and educational efforts related to OT</td></tr>
<tr><td rowspan="3">Required qualifications</td><td>Education</td><td>Bachelor’s degree in computer science, computer engineering or related discipline or equivalent training and experience.</td></tr>
<tr><td>Training</td><td>Specialized training associated with OT cybersecurity as well as system specific tools and techniques required.</td></tr>
<tr><td>Work experience</td><td>Preferred experience for entry level role requires moderate experience 2-3 years working in the OT environment.</td></tr>
<tr><td>Tools & Technology</td><td colspan="2">▪ Strategic and business plans
▪ Threat and risk assessments
▪ OT Vulnerability management processes and vulnerability assessments
▪ Incident management processes and procedures
▪ Security event and incident management systems and/or incident reporting systems and networks that may be used for OT cybersecurity incidents,
▪ Cybersecurity risk management processes & policies
▪ Privacy and security legislation
▪ Organizational security infrastructure and reporting systems
▪ OT security tools, techniques and procedures</td></tr>
<tr><td>Competencies</td><td colspan="2">Appreciating that not all OT analysts will necessarily have an IT background, the following basic application of the following KSAs are relevant:

☐ Telemetry systems, data communications, data acquisition and process control
☐ Operating systems, networking, and communications systems concepts
☐ Electrical distribution networks, power system equipment, transformer station operation and electrical theory
☐ Computer and networking troubleshooting and maintenance procedures
☐ Network administration principles and practices
☐ System life cycle management principles, including software security and usability
☐ Database management systems and applications;
☐ Database administration and optimization
☐ System testing and evaluation methodologies and processes
☐ Measures or indicators of system performance, availability, capacity, or configuration problems
☐ Analysis tools and network protocols
☐ Diagnostic tools and fault identification techniques

Advanced application of the following KSAs:

☐ OT systems software and hardware, programmable logic controllers, and digital and analog relaying;
☐ Threat and risk assessment to internet connected OT (including implications and assessment of IoT devices)</td></tr>
</table>

	☐ Legal and compliance requirements including organizational responsibilities for workplace and public safety related to OT/ production ☐ Industry standards and best practices, especially related to industrial environments in the cybersecurity space ☐ Cybersecurity program management, measures and monitoring Control systems – applicable to industry/production environments ☐ IT/OT integration and convergence ☐ Process safety and hazard analysis ☐ Systems analysis and integration ☐ Problem-solving in complex systems environments ☐ Technical communications including report writing to address cross- disciplinary technical issues
Future Trends Affecting Key Competencies	▪ The increased reliance on virtualized and/or 'cloud-based' services will require knowledge of responsibilities of the services provider including their cybersecurity responsibilities relative to organizational cybersecurity risks and specifically those that relate to OT and remote operation and access. ▪ If practiced within the organization, there will be a requirement to fully understand the security implications of 'bring your own devices' (BYOD) and remote monitoring and operations through IoT and devices. ▪ Increased use of automated tools, aided by artificial intelligence, will require understanding of how the tools will be integrated into the organizational security infrastructure and the implications to OT requirements, procedures, and policies. ▪ Increased use of automated tools by threat actors pose challenges for organizations that do not have complementary defensive tools. Accordingly, creative, locally relevant mitigation strategies will be required. ▪ Mechanisms to support the required level of trust and organizational risk will need to be in place to support monitoring and reporting of results from automated tools. Consequently, there will be a need to understand organizational risks posed, measures of security and what policies, processes, or procedures need to be in place. ▪ The emergence and use of quantum technologies by threat actors will fundamentally change encryption security. For encryption within OT systems, this will require knowledge and skills related to implementing a quantum safe strategy within the organization.

Supply Chain Security Analyst

NICE Framework Reference	None.
Functional Description	Has the primary responsibility to collect and analyze data to identify cybersecurity flaws and vulnerabilities in an organization's supply chain operations, and to provide advice and guidance to help reduce these supply chain risks.
Consequence of error or risk	Error, neglect, outdated information or poor judgment could result in organizational decisions that can have a significant impact on the business. Lack of a full appreciation of the business needs for security will jeopardize the security posture of the organization in the face of evolving threats.
Development pathway	Typically drawn from cybersecurity analysis roles (e.g. Cybersecurity operations analyst, vulnerability analyst, etc.) this role can nonetheless be assumed by a broad cross-section of professionals who can assess and provide insights on the potential supply chain threats. This includes those who may specialize in human factors aspects of supply chain (e.g. close access, insider threat).
Other titles	Cybersecurity analyst Supply chain integrity analyst
Related NOCs	2171 Information systems analysts and consultants 2174 Computer programmers and interactive media developers
Tasks	▪ Collaborate with key stakeholders to establish an effective cybersecurity risk management program ▪ Ensure compliance with the changing laws and applicable regulations ▪ Develop and implement plans that are aligned to the organizational objectives and security requirements ▪ Collect and analyze supply chain relevant information to identify and mitigate flaws and vulnerabilities, including component integrity, in an organization's computer networks or systems ▪ Analyze system hardware and software configurations ▪ Recommend hardware, software, and countermeasures to install or update based on cyber threats and security vulnerabilities ▪ Coordinate with colleagues to implement changes and new systems ▪ Track and report on cyber threats and security vulnerabilities that impact supply chain performance ▪ Define, develop, implement, and maintain cybersecurity plans, policies and procedures ▪ Ensure compliance with cybersecurity policies, regulations, and procedures of the organization ▪ Ensure compliance with security requirements of organization networks and systems ▪ Develop and maintain risk assessments and related reports on vendors, products and services ▪ Define and maintain tool sets and procedures that support supply chain integrity ▪ Prepare technical reports

	▪ Develop, deliver, and oversee related cybersecurity training material and educational efforts related to cybersecurity and supply chain integrity	
Required qualifications	Education	Post-secondary education in a cyber or IT related field (e.g.; Computer engineering, Computer Science, Information Technology, Business Technology Management – Digital Security or equivalent)
	Training	In addition to formal training in cybersecurity analysis, specialized training and skills in vulnerability analysis and supply chain threats required.
	Work experience	Individuals employed in this role can have diverse levels of cybersecurity expertise. Requested experience will depend on the organizational need and complexity of systems to be analyzed.
Tools & Technology	▪ Strategic and business plans ▪ Threat and risk assessments ▪ Vulnerability management processes and vulnerability assessment tools and applications ▪ Incident management processes and procedures ▪ Organizational security infrastructure and reporting systems Security event and incident management systems and/or incident reporting systems and networks, ▪ Cybersecurity risk management processes & policies across the supply chain ▪ Third party and service level agreements and contracts	
Competencies	Basic application of the following KSAs: ☐ Integrated/organizational security concepts, principles and practice (software, system, data, physical and personnel) ☐ Preventative technical, operational and management controls available and organizational responsibilities for those controls ☐ Sector/context relevant threats, business needs and technical infrastructure ☐ Project management and security requirements throughout the project lifecycle ☐ Procurement processes and security requirements Advanced application of the following KSAs: ☐ Organizational security infrastructure including protective and defensive systems across the supply chain ☐ Cybersecurity threat landscape and threat intelligence sources for supply chain threats ☐ Legal and compliance requirements as they extend to organizational third-party arrangements ☐ Vulnerability analysis and tools ☐ Advanced security information and data security analysis and techniques ☐ Functional and technical design of networks and system, and cybersecurity solutions ☐ Risk management processes, responsibilities and authorities within the organization and across the supply chain ☐ Third party risk management and liability	

	☐ System life cycle management principles, including software security and usability ☐ Current national supply chain processes
Future Trends Affecting Key Competencies	▪ The increased reliance on virtualized and/or 'cloud-based' services will require knowledge of responsibilities of the services provider including their cybersecurity responsibilities relative to organizational cybersecurity risks. ▪ If practiced within the organization, there will be a requirement to fully understand the security implications of 'bring your own devices' (BYOD) and managing the associated risks. ▪ Increased use of automated tools, aided by artificial intelligence, will require understanding of how the tools will be integrated into the organizational security infrastructure and the implications to personnel, resources, procedures, and policies. ▪ Increased use of automated tools by threat actors pose challenges for organizations that do not have complementary defensive tools. Accordingly, creative, locally relevant mitigation strategies will be required. ▪ Mechanisms to support the required level of trust and organizational risk will need to be in place to support monitoring and reporting of results from automated tools. Consequently, there will be a need to understand organizational risks posed, measures of security and what policies, processes, or procedures need to be in place. ▪ The emergence and use of quantum technologies by threat actors will fundamentally change encryption security. This will require knowledge and skills related to implementing a quantum safe strategy within the organization.

Information Systems Security Developer

NICE Framework Reference	Securely Provision, SP-SYS-001, Information Systems Security Developer
Functional Description	Develops, creates, integrates, tests, and maintains information system security throughout the systems life cycle, and reports on information system performance in providing confidentiality, integrity, and availability and recommends corrective action to address deficiencies.
Consequence of error or risk	Error, neglect, outdated information or poor judgment could result in organizational decisions that can have a significant impact on the business. Lack of a full appreciation of the business needs for security will jeopardize the security posture of the organization in the face of evolving threats.
Development pathway	This is an entry level role in cybersecurity that leverages previous IT and systems experience, following cybersecurity technical training, this work can lead to increased responsibilities in cybersecurity infrastructure roles and technical expertise.
Other titles	IT Security Systems Administrator Cybersecurity systems technician
Related NOCs	2171 Information systems analysts and consultants 2174 Computer programmers and interactive media developers
Tasks	▪ Collaborate with key stakeholders to establish an effective cybersecurity risk management program ▪ Ensure compliance with the changing laws and applicable regulations ▪ Define and review an organization's information systems, and ensure security requirements recognize appropriate disaster recovery plans and business continuity functions, including any failover or backup requirements for system restoration ▪ Analyze existing security systems and make recommendations for changes or improvements ▪ Prepare cost estimates and constraints, and identify integration issues or risks to organization ▪ Research and develop a system security context, and define security assurance requirements based on industry standards and cybersecurity policies and practices ▪ Ensure the acquired or developed systems are consistent with an organization's cybersecurity policies and practices ▪ Develop and conduct information system testing and validation procedures and report on functionality and resiliency ▪ Plan and support vulnerability testing and security reviews on information systems or networks to identify gaps, and examine controls and measures required to protect the confidentiality and integrity of information under different operating conditions ▪ Conduct trial runs of information systems to ensure security levels and procedures are correct and develop a security risk management plan; ▪ Support development of disaster recovery and continuity of operations plans for information systems under development ▪ Prepare technical reports that document system development process and subsequent revisions

	▪ Document and address security throughout a system life cycle; ▪ Update and upgrade information systems as needed to correct errors, and to improve performance and interfaces ▪ Prepare reports on information systems patches or releases that would leave networks or systems vulnerable ▪ Develop countermeasures and risk mitigation strategies against potential exploitations of vulnerabilities in networks or systems ▪ Perform risk analysis whenever a system undergoes a change ▪ Develop, deliver, and oversee related cybersecurity training material and educational efforts related to role	
Required qualifications	Education	Post-secondary education in a cyber or IT related field (e.g., Computer Science, IT systems administration, Computer Engineering or equivalent).
	Training	Supporting training can include cybersecurity systems development tools, techniques and practices as well as Security throughout the system development lifecycle
	Work experience	Previous training and experience in system development.
Tools & Technology	▪ Strategic and business plans ▪ Threat and risk assessments ▪ Vulnerability management processes and vulnerability assessments ▪ Incident management processes and procedures ▪ Security event and incident management systems and/or incident reporting systems and networks, ▪ Cybersecurity risk management processes & policies ▪ Privacy and security legislation ▪ Organizational security infrastructure and reporting systems	
Competencies	Underpinning this occupation are those competencies demonstrated for an executive level which include those identified within the NICE framework. Basic application of the following KSAs: ☐ Integrated/organizational security concepts, principles and practice (software, system, data, physical and personnel) ☐ Risk management policies, requirements, and practices; ☐ Business continuity and disaster response planning; ☐ Preventative technical, operational and management controls available and organizational responsibilities for those controls ☐ Sector/context relevant threats, business needs and technical infrastructure ☐ Project management ☐ Costing models and cost benefit analysis ☐ Cryptography and cryptographic key management concepts; ☐ Identity and access management ☐ Vulnerability management and penetration testing planning and processes ☐ Data security conceptions and functions, analysis methodologies, testing, and protocols ☐ Secure coding and configuration techniques ☐ Cybersecurity program management, measures and monitoring	

	Advanced application of the following KSAs: ☐ Industry standards and organizationally accepted system analysis principles and methods ☐ System design tools, methods, and techniques ☐ Computer architecture, data structures, and algorithms ☐ System life cycle management principles, including software security and usability ☐ System testing and evaluation methodologies and processes; ☐ System, application and data security threats, risks and vulnerabilities; ☐ Designing countermeasures to identified security risks; ☐ Configuring and using software-based computer protection tools ☐ Considerations for designing and hardware and software solutions ☐ Incident management and system recovery
Future Trends Affecting Key Competencies	▪ The increased reliance on virtualized and/or 'cloud-based' services will require knowledge of responsibilities of the services provider including their cybersecurity responsibilities and system to system interactions, access and accountabilities. ▪ If practiced within the organization, there will be a requirement to fully understand the security implications of 'bring your own devices' (BYOD) and managing the associated risks throughout the system development life-cycle. ▪ Increased use of automated tools, aided by artificial intelligence, will require understanding of how the tools will be integrated into the organizational security infrastructure. ▪ Increased use of automated tools by threat actors pose challenges for organizations that do not have complementary defensive tools. Accordingly, creative, locally relevant mitigation strategies will be required, and system security responses developed and exercised. ▪ Mechanisms to support the required level of trust and organizational risk will need to be in place to support monitoring and reporting of results from automated tools. Consequently, there will be a need to understand organizational risks posed, measures of security and what policies, processes, or procedures need to be in place. ▪ The emergence and use of quantum technologies by threat actors will fundamentally change encryption security. This will require knowledge and skills related to implementing a quantum safe strategy within the organization and across all systems that handle sensitive data.

Security Automation Engineer/Analyst

NOTE: *This is an emerging work role. There are limited samples of this work role and subject matter expert tasks and activities vary based on organizational requirements. Accordingly, the information below is based upon current representations based on demand driven requirements and an understanding of artificial intelligence, machine learning and data science requirements to support automated process engineering and analysis*. *It is anticipated that this will evolve significantly over the next years.*

NICE Framework Reference	None.
Functional Description	Given references, organizational security documentation, IT security guidance and required tools and resources researches and defines the business needs for security, identifies requirements for and engineers automated solutions that support organizational security.
Consequence of error or risk	Error, neglect, outdated information or failure to account for organizational requirements, business needs and threats could result in poor systems design and/or integration of systems/devices that create exploitable vulnerabilities which can have significant implications to organizational objectives including the potential for catastrophic systems failure.
Development pathway	Typically follows formal education and 5-10 years' experience in related IT engineering, systems design, or systems integration functions. Additional training, education and/or experience in process automation and related artificial intelligence/machine learning engineering activities.
Other titles	▪ Systems automation engineer ▪ Automated systems designer ▪ Security automation and controls engineer
Related NOCs	2133 Electrical and electronics engineers 2147 Computer engineers (except software engineers and designers) 2173 Software engineers and designers 2241 Electrical and electronics engineering technologists and technician
Tasks	▪ Research, develop, integrate, test and implement security automation solutions for cloud or systems ▪ Scope and plan out automation work to meet timelines ▪ Manage/monitor automated security solution activities including fixes, updates and related processes ▪ Develop and maintain tools and processes to support security automation activities ▪ Review and test security automation scripting prior to implementation ▪ Troubleshoot any issues that arise during testing, production or use ▪ Create, use and maintain resource documentation for reference ▪ Identify, acquire and oversee management of financial, technical and personnel resources required to support security automation activities ▪ Review, approve, and oversee changes on cybersecurity policies and controls and their implication for automated activities ▪ Schedule and oversee security assessments and audits ▪ Oversee and manage vendor relations related to acquired IT security products and services ▪ Ensure security requirements are identified for all IT systems throughout their life cycle

<table>
<tr><td></td><td colspan="2">▪ Supervise or manage protective or corrective measures when a cybersecurity incident or vulnerability is discovered.
▪ Assess threats and develop countermeasures and risk mitigation strategies against automated system vulnerabilities
▪ Perform risk analysis and testing whenever an automated system undergoes a change
▪ Develop, deliver, and oversee related cybersecurity training material and educational efforts related to role</td></tr>
<tr><td rowspan="3">Required qualifications</td><td>Education</td><td>Relevant engineering or computer science degree with post graduate training or equivalent in systems automation, artificial learning or machine learning.</td></tr>
<tr><td>Training</td><td>Relevant cybersecurity training to support functions as a security engineer.</td></tr>
<tr><td>Work experience</td><td>Moderate experience (3-5 years) in security and associated systems design, integration, testing and support. Experience in programming and application testing. 2-3 years practical experience in automating system processes.</td></tr>
<tr><td>Tools & Technology</td><td colspan="2">▪ Threat and risk assessment tools and methodologies
▪ Protective and defensive systems including firewalls, anti-virus software and systems, intrusion detection and protection systems, scanners and alarms
▪ Security event and incident management systems and/or incident reporting systems and networks
▪ Authentication software and systems
▪ Vulnerability management processes and vulnerability assessment systems including penetration testing if used
▪ Security services provided if applicable
▪ Security testing and evaluation tools and techniques
▪ Process automation tools, techniques and procedures
▪ Applicable programming languages</td></tr>
<tr><td>Competencies</td><td colspan="2">Advanced level of application of the following KSAs:
☐ Process automation within a security setting
☐ API, automation and scripting languages
☐ SDN, NFV, and VNF functions
☐ Security engineering models
☐ Defining and communicating security approaches that support organizational requirements
☐ International security standards and compliance
☐ Security architecture concepts and enterprise architecture reference models
☐ Systems security during integration and configuration
☐ Security assessment and authorization processes
☐ Security testing and evaluation methodologies and processes
☐ Security across the system / software development lifecycle
☐ Vulnerability assessment and penetration testing methodologies and applications
☐ Systems and software testing and evaluation methodologies
☐ Evidence-based security design
☐ Developing and testing threat models
☐ Project management and security assessment throughout the project lifecycle
☐ Procurement processes and supply chain integrity assessments</td></tr>
</table>

	☐ Advising on security requirements, policies, plans and activities ☐ Drafting and providing briefings and reports to different audience levels (users, managers, executives)
Future Trends Affecting Key Competencies	▪ The increased reliance on virtualized and/or 'cloud-based' services will require knowledge of responsibilities of the services provider including their cybersecurity responsibilities relative to organizational cybersecurity risks. ▪ If practiced within the organization, there will be a requirement to fully understand the security implications of 'bring your own devices' (BYOD) and managing the associated risks. ▪ If automated security tools will be used, testing, integration and monitoring requirements will need to be defined and those responsible for these activities will need to be advised / trained on the resulting process and procedural changes. Additionally, as the potential technical lead for security automation, there may be a requirement to educate organizational leaders on the benefits and risks of automation and any change management required. ▪ Increased use of automated tools by threat actors pose challenges for organizations that do not have complementary defensive tools. Accordingly, creative, locally relevant mitigation strategies will be required. This will require a significantly better appreciation of threat actor capabilities and potential countermeasures. ▪ Mechanisms to support the required level of trust and organizational risk will need to be in place to support monitoring and reporting of results from automated tools. Consequently, there will be a need for increased understanding of organizational risks posed within the dynamic threat environment. ▪ The emergence and use of quantum technologies by threat actors will fundamentally change encryption security. This will require knowledge and skills related to implementing a quantum safe strategy and understanding of the implications on AI-enabled security mechanisms.

Cryptographer/Cryptanalyst

NICE Framework Reference	None.	
Functional Description	Develops algorithms, ciphers, and security systems to encrypt information/Analyzes and decodes secret messages and coding systems.	
Consequence of error or risk	Error, neglect, outdated information or poor judgment could result in poor cryptologic artefacts, protocols, and systems that will jeopardize intended security of the systems / information they are protecting. Failure to keep up to date on related science and emerging technology carries equal risk.	
Development pathway	A highly specialized cybersecurity activity, this role is filled by experienced and educated professionals who are interested in this field. Opportunities exist for increased specialization and advanced research and studies in the field.	
Other titles	None.	
Related NOCs	2147 Computer engineers (except software engineers and designers) 2161 Mathematicians, statisticians and actuaries 2171 Information systems analysts and consultants	
Tasks	▪ Collaborate with key stakeholders to establish an effective cybersecurity risk management program ▪ Ensure compliance with the changing laws and applicable regulations ▪ Develop systems for protection of important/sensitive information from interception, copying, modification and/or deletion ▪ Evaluate, analyze and target weaknesses and vulnerabilities in security systems and algorithms ▪ Develop statistical and mathematical models to analyze data and troubleshoot security problems ▪ Develop and test computational models for reliability and accuracy ▪ Identify, research and test new cryptology theories and applications ▪ Decode cryptic messages and coding systems for the organization ▪ Develop and update methods for efficient handling of cryptic processes ▪ Prepare technical reports that document security processes or vulnerabilities ▪ Provide guidance to management and personnel on cryptical or mathematical methods and applications ▪ Support countermeasures and risk mitigation strategies against potential exploitations of vulnerabilities related to cryptographic systems and, algorithms ▪ Provide insights and guidance related to quantum safety and quantum resistant strategies ▪ Support incident management and post-analysis in the event of a compromise to encryption/cryptographic processes or systems ▪ Develop, deliver, and oversee related cybersecurity training material and educational efforts related to role ▪ Guide and support encryption specialists as required	
Required qualifications	Education	Post-secondary university degree in Computer Engineering, Computer Science, or Mathematics. A Master of Science or Doctorate is preferred.

	Training	As required to support organizational technical context (e.g. local tools, processes and procedures)
	Work experience	In addition to academic credentials, entry level roles normally require 3-5 years' experience in an IT/systems domain with familiarity of encryption and key management activities.
Tools & Technology	▪ Threat and risk assessments ▪ Vulnerability management processes and vulnerability assessments ▪ Incident management processes and procedures (crypto/encryption related) ▪ Cybersecurity risk management processes & policies ▪ Privacy and security legislation ▪ Cryptographic algorithms, ciphers and systems ▪ Key management policies and plans ▪ Organizational security infrastructure and reporting systems	
Competencies	Underpinning this occupation are those competencies demonstrated for an executive level which include those identified within the NICE framework. Basic application of the following KSAs: ☐ Integrated/organizational security concepts, principles and practice (software, system, data, physical and personnel) ☐ Preventative technical, operational and management controls available and organizational responsibilities for those controls ☐ Sector/context relevant threats, business needs and technical infrastructure ☐ Information and data requirements including sensitivity, integrity and lifecycle ☐ Applicable computer programming languages ☐ Cybersecurity program management, measures and monitoring Advanced application of the following KSAs: ☐ Advanced threats and crypto breaking /decryption capabilities ☐ Applicable laws, legal codes, regulations, policies and ethics as they relate to cybersecurity; and ☐ Computer architecture, data structures, and algorithms ☐ Linear/matrix algebra and/or discrete mathematics ☐ Probability theory, information theory, complexity theory and number theory ☐ Cryptography and cryptographic key management concepts; ☐ Principles of symmetric cryptography (e.g., symmetric encryption, hash functions, message authentication codes, etc.) ☐ Principles of asymmetric cryptography (asymmetric encryption, key exchange, digital signatures, etc.) ☐ Incident response requirements for cryptographic compromise ☐ Technical report writing	
Future Trends Affecting Key Competencies	▪ The increased reliance on virtualized and/or 'cloud-based' services will require knowledge of responsibilities of the services provider including their cybersecurity responsibilities relative to organizational cybersecurity risks particularly as they pertain to data encryption requirements. ▪ Increased use of automated tools, aided by artificial intelligence, will require understanding of how the cryptographic tools are affected and automated to support organizational requirements.	

	▪ Increased use of automated tools by threat actors pose challenges for organizations that do not have complementary defensive tools to ensure robust cryptographic systems, ciphers and algorithms. If there are known disparities between the threat and the ability to defend, mitigations should be defined and implemented ▪ Mechanisms to support the required level of trust and organizational risk will need to be in place to support monitoring and reporting of results from automated tools. Consequently, there will be a need to understand organizational risks posed, measures of security and what policies, processes, or procedures need to be in place. ▪ The emergence and use of quantum technologies by threat actors will fundamentally change encryption security. This will require knowledge and skills related to implementing a quantum safe strategy within the organization. The cryptographer/cryptanalyst will play a key role in ensuring quantum safe/resistant design and may be involved in testing of algorithms, encryption protocols and equipment.

Operate & Maintain

This activity area/work category is involved in operating and maintaining system and data security as prescribed within the security architecture and design specifications. All these functions are performed within existing occupations within the Canadian labour market with the exception of those identified below which have become established as occupations with the increasing reliance on internet connected systems and associated threats.

- Identity and Authentication Management Support Specialist
- Encryption/ Key Management Support Specialist
- Data Privacy Specialist / Privacy Officer

For the cybersecurity specialist working in this activity area, not only do they need to bring their technical expertise, they are also required to closely integrate with day-to-day organizational IT operational requirements. This typically involves enhanced client-services and communication skills in addition to the technical competencies.

Identity Management & Authentication Support Specialist

NICE Framework Role	None.	
Functional Description	Provides ongoing support to identity, credentials, access and authentication management in support of organizational IT security.	
Consequence of error or risk	Error, neglect, outdated information, lack of attention to detail or poor judgment could result in compromise of the system which, depending on the type of compromise, may have a significant impact on organizational IT systems, capabilities or functions.	
Development pathway	This is an often an entry-level job to the security domain after gained experience with network or system administration access management and credentials. With additional training and experience there is potential for more technically or operationally focused roles as well as management opportunities.	
Other titles	▪ Access management analyst ▪ System analyst ▪ Identity, credentials and access management (ICAM) specialist	
Related NOCs	2171 Information systems analysts and consultants 2281 Computer network technicians 2282 User support technicians	
Tasks	▪ Identify client requirements and propose technical solutions ▪ Model and map users to resources (e.g. role based) ▪ Install, configure, operate, maintain and monitor related applications ▪ Deploy, configure and manage user provisioning including identity synchronization, auto-provisioning and automatic access deactivation, self-service security request approvals workflow and consolidated reporting ▪ Configure and manage enterprise and web-based access management solutions (single sign on, password management, authentication & authorization, delegated administration) ▪ Analyze patterns or trends in incidents for further resolution ▪ Manage identity change-request approval processes ▪ Audit, log and report user life-cycle management steps against access control list on managed platforms ▪ Configure and manage federated identity, credentials, access management tools in compliance with security policy, standards and procedures ▪ Complete tasks related to authorization and authentication in physical and logical environments ▪ Develop, deliver, and oversee related cybersecurity training material and educational efforts related to role	
Required qualifications	Education	College diploma in IT field.
	Training	Training in relevant identity, credentials, access management and authentication policies, protocols, tools and procedures. Developing and applying user credential management system.
	Work experience	Experience in managing directory services and working in a security environment.

Tools & Technology	▪ Identity and access management systems ▪ Directory services ▪ Authentication tools and services ▪ Security event and incident management systems and/or incident reporting systems and networks
Competencies	KSAs applied at the basic level: ☐ Identity, credential and access management architectures and standards ☐ Related application life-cycle processes ☐ Mapping and modeling credentials ☐ Policy-based and risk-adaptive access controls ☐ Developing and applying user credential management system ☐ Organizational analysis of user and business trends ☐ Client consultation and problem resolution KSAs applied at an advanced level: ☐ Network access, identity, and access management protocols, tools and procedures ☐ Authentication, authorization, and access control methods ☐ Install, configure, operate, maintain and monitor related applications ☐ Developing and applying security system access controls. ☐ Maintaining directory services ☐ Organizational information technology (IT) user security policies (e.g., account creation, password rules, access control)
Future Trends Affecting Key Competencies	▪ The increased reliance on virtualized and/or 'cloud-based' services will require knowledge of responsibilities of the services provider including their responsibilities for cybersecurity systems management. ▪ If practiced within the organization, there will be a requirement to fully understand the implications of 'bring your own device' (BYOD) policies. This means that regardless of the device capabilities, there will need to be an assessment of the risks posed to the organization, mitigations to account for potential compromise through a personal device, and what actions will be required by the SOC in the event of an incident. ▪ Increased use of automated tools, aided by artificial intelligence, will require understanding of how the tools will be integrated into identity and access management processes and the related technical and process changes. ▪ Mechanisms to support the required level of trust and organizational risk will need to be in place to support monitoring and reporting of results from automated tools. Consequently, there will need to be increased understanding of organizational risks posed and potential responses within the dynamic threat environment. ▪ The emergence and use of quantum technologies by threat actors will fundamentally change encryption security. This will require knowledge and skills related to implementing a quantum safe strategy as well as a deep understanding of the implications to authentication protocols and how to defend against potential quantum computing threats.

Encryption / Key Management Support Specialist

NICE Framework Reference	None.	
Functional Description	Provides ongoing support to management and maintenance of virtual private networks, encryption, public key infrastructure, and, in some cases, Communications Security (COMSEC) in support of organizational IT security.	
Consequence of error or risk	Error, neglect, outdated information, lack of attention to detail or poor judgment could result in compromise of the system which, depending on the type of compromise, may have a significant impact on organizational IT systems, capabilities or functions.	
Development pathway	This is an often an entry-level job to the security domain after gained experience with network or system administration access management and credentials. With additional training and experience there is potential for more technically or operationally focused roles as well as management opportunities.	
Other titles	▪ Access management analyst ▪ System analyst ▪ Identity, credentials and access management (ICAM) specialist	
Related NOCs	2171 Information systems analysts and consultants 2281 Computer network technicians 2282 User support technicians	
Tasks	▪ Identify client requirements and propose technical solutions ▪ Install, configure, operate, maintain and monitor related applications ▪ Developing and applying security system access controls ▪ Deploy, configure and manage encryption/key management services ▪ Establish VPNs ▪ Analyze patterns or trends for further resolution ▪ Manage identity change-request approval processes ▪ Audit, log and report user life-cycle management steps against access control list on managed platforms ▪ Configure and manage federated identity, credentials, access management tools in compliance with security policy, standards and procedures ▪ Complete tasks related to authorization and authentication in physical and logical environments ▪ Develop, deliver, and oversee related cybersecurity training material and educational efforts related to role	
Required qualifications	Education	College diploma in IT field.
	Training	Training in relevant encryption and key management technologies at the applied level.
	Work experience	Experience in managing directory services and working in a security environment.
Tools & Technology	▪ Identity and access management systems ▪ Encryption and key management tools, processes and procedures ▪ VPN and Wi-fi encryption tools and procedures ▪ Authentication tools and services ▪ Security event and incident management systems and/or incident reporting systems and networks	
Competencies	KSAs applied at the basic level:	

	☐ Cryptanalysis ☐ Cryptography and encryption concepts and methodologies ☐ Symmetric and asymmetric cryptography ☐ Steganography and Steganalysis ☐ National cryptologic authorities (Communications Security Establishment) ☐ Public key infrastructure providers KSAs applied at the advanced level: ☐ Organizational information technology (IT) user security policies (e.g., account creation, password rules, access control) ☐ Network access, identity, and access management protocols, tools and procedures ☐ National and international standards ☐ Authentication, authorization, and access control methods ☐ PKI (Public Key Infrastructure), HSM (Hardware Security Module), Digital Certificate, SSL/TLS (Secure Sockets Layer / Transport Layer Security), SSH (Secure Shell), current encryption technologies ☐ Related application life-cycle processes ☐ Digital signatures, digital certificates, and digital certificate management ☐ Authentication protocols ☐ VPN and Protocols ☐ File and Disk Encryption ☐ Encryption Algorithms ☐ Organizational analysis of user and business trends ☐ Client consultation and problem resolution
Future Trends Affecting Key Competencies	▪ The increased reliance on virtualized and/or 'cloud-based' services will require knowledge of responsibilities of the services provider including their cybersecurity responsibilities relative to organizational cybersecurity risks particularly as they pertain to data encryption requirements. ▪ Increased use of automated tools, aided by artificial intelligence, will require understanding of how the cryptographic tools are affected and automated to support organizational requirements. ▪ Increased use of automated tools by threat actors pose challenges for organizations that do not have complementary defensive tools to ensure robust cryptographic systems, ciphers and algorithms. If there are known disparities between the threat and the ability to defend, mitigations should be defined and implemented ▪ Mechanisms to support the required level of trust and organizational risk will need to be in place to support monitoring and reporting of results from automated tools. Consequently, there will be a need to understand organizational risks posed, measures of security and what policies, processes, or procedures need to be in place. ▪ The emergence and use of quantum technologies by threat actors will fundamentally change encryption security. This will require knowledge and skills related to implementing a quantum safe strategy within the organization. This includes knowledge and skill of quantum safe algorithms being used, integration and implementation of quantum safe technologies within the

	organization and testing and evaluation protocols for quantum safe/quantum resistant hardware, software, and protocols.

Data Privacy Specialist/Privacy Officer

NICE Framework Reference	Oversee and Govern, OV-LGA-002, Privacy Officer/Privacy Compliance Manager
Functional Description	Develops, implements, advises on and administers organization privacy compliance program which supports requirements to safeguard personal private information (PPI).
Consequence of error or risk	Error, neglect, outdated information, lack of attention to detail or poor judgment could result in a compromise or breach of PPI, which, in addition to the potential individual consequences and liability, may result in significant fines levied for the breach, and loss of reputation and trust.
Development pathway	This role may be supported through technical or non-technical pathways that lead to an entry level role related to privacy/sensitive data management and progress to the policy advisor level. Individuals can further specialize in data security or policy analyst, or senior advisor.
Other titles	▪ Privacy officer ▪ Privacy compliance officer/manager
Related NOCs	2171 Information systems analysts and consultants 416X Policy and program researchers, consultants and officers (context dependent)
Tasks	▪ Interpret and apply laws, regulations, policies, standards, or procedures to specific privacy issues ▪ Conduct periodic impact assessments and ongoing compliance monitoring activities to identify compliance gaps and/or areas of risk to ensure privacy concerns, requirements and responsibilities are addressed ▪ Establish and maintain a mechanism to track access to information within the purview of the organization and as required by law to allow qualified personnel to review or receive such information ▪ Establish and implement an internal privacy audit program, and prepare audit reports that identify technical and procedural findings, and privacy violations, and recommend remedial solutions ▪ Provide advice and guidance on laws, regulations, policies, standards, or procedures to management, personnel, or key departments ▪ Ensure compliance with privacy and cybersecurity laws, regulations, and policies, and consistent application of sanctions for failure to comply with stated measures for all personnel in the organization ▪ Initiate, facilitate and promote activities to foster privacy awareness within the organization that include the collection, use and sharing of information ▪ Monitor advancements in privacy enhancing technology and ensure the use of technologies complies with privacy and cybersecurity requirements, including the collection, use and disclosure of information ▪ Review the organization's network security plans and projects to ensure that they are consistent with privacy and cybersecurity goals and policies ▪ Collaborate with legal counsel and management to ensure the organization has and maintains appropriate privacy and confidentiality consent, authorization forms, and relevant materials are compliant with legal practices and requirements

	▪ Develop, deliver, and oversee privacy training material and awareness activities	
Required qualifications	Education	Post-secondary education in an applicable field (e.g.; Business Administration, Law, Political Science, Social Sciences or equivalent)
	Training	Specialized training in data privacy and security, cybersecurity foundations, privacy impact analysis, privacy legislation and compliance
	Work experience	Previous training and experience (2-3 years) in policy analysis role related to security or privacy typically required for entry level role
Tools & Technology	▪ Privacy and information legislation and policies ▪ Compliance requirements ▪ Reporting mechanisms and templates ▪ Privacy impact assessments/statements of sensitivity ▪ Threat and risk assessments ▪ Data and information requirements ▪ Privacy assessment tools and methodologies	
Competencies	KSAs applied at the basic level: ☐ A working knowledge of cybersecurity principles and elements ☐ Technical knowledge to understand data security and integrity, security requirements, and the functional and technical design of networks and system, and cybersecurity solutions ☐ Data security conceptions and functions, analysis methodologies, testing, and protocols ☐ Cybersecurity program management, measures and monitoring KSAs applied at an advanced level: ☐ Threat and risk assessment (focused on privacy / data privacy security) ☐ Domestic and international laws, regulations, policies, and procedures; ☐ Information security policies, procedures, and regulations ☐ Specific impacts of cybersecurity gaps and breaches ☐ Monitor advancements in privacy laws and policies ☐ Privacy impact assessments ☐ Privacy disclosure statements based on laws and regulations ☐ Breach reporting	
Future Trends Affecting Key Competencies	▪ The increased reliance on virtualized and/or 'cloud-based' services will require knowledge of responsibilities of the services provider including their responsibilities for protecting sensitive data and responding/reporting potential breaches ▪ Increased use of automated tools, aided by artificial intelligence, will require understanding of how the tools will be integrated into protection of PPI within the organization and how that needs to be translated into policies, procedures and practices. ▪ Increased use of automated tools by threat actors will likely challenge existing technologies and resources intended to manage protection of PPI. Accordingly, additional tools, processes or training will be required to stay ahead of the threats. ▪ Mechanisms to support the required level of trust and organizational risk will need to be in place to support monitoring and reporting of results from automated tools. Consequently, there will be a need to	

	understand organizational risks posed to PPI/data, measures of security and what policies, processes, or procedures need to be in place. ▪ The emergence and use of quantum technologies by threat actors will fundamentally change encryption security. Encryption used to protect PPI will require knowledge and skills related to ensuring that the PPI remains protected under quantum threat.

Protect & Defend

This occupational sub-group area is involved with cybersecurity operations that encompass active protection, event detection, incident response and recovery of organizational digital systems. While individuals have been doing related jobs for decades, the key work roles have not been identified as occupations but rather have been typically associated with occupational groups: computer and information systems managers (NOC 0213); information systems analysts and consultants (2171); and information systems testing technicians (2283). Individuals in this, the Protect & Defend work area, are therefore focused on managing cybersecurity technologies, processes and personnel, that requires unique experience and distinct knowledge, skills and abilities that differentiate them from their other technical colleagues.

The following occupations have been more clearly defined as supporting cybersecurity operations.

- Information Systems Security Manager – Cybersecurity Operations
- Cybersecurity Operations Analyst (a.k.a. in the NICE framework as a Cyber Defense Analyst)
- Cybersecurity Operations Infrastructure Support Specialist (a.k.a. in the NICE framework as a Cyber Defense Infrastructure Support Specialist)
- Cybersecurity Incident Responder (a.k.a. in the NICE framework as a Cyber Defense Incident Responder)
- Cybersecurity Operations Technician
- Vulnerability Assessment Analyst
- Penetration Tester
- Digital Forensics Analyst (a.k.a. in the NICE framework as a Cyber Defense Digital Forensics Analyst)

Information Systems Security Manager - Cybersecurity Operations

NICE Framework Reference	Oversee & Govern, OV-MGT-001, Information Systems Security Manager,	
Functional Description	Plans, organizes, directs, controls and evaluates the activities of the cybersecurity operations centre within an organization. Employed throughout the public and private sectors.	
Consequence of error or risk	Error, neglect, outdated information or poor judgment could result in catastrophic failure of organizational IT and data systems and associated implications to the organizational functions which rely on those systems.	
Development pathway	Typically follows 5 to 10 years in related roles in IT operations or cybersecurity operations or similar employment. This role supports increasing management level responsibilities based on a solid technical foundation in cybersecurity operations or a related work role (e.g. vulnerability assessment & management, digital forensics, cybersecurity analysis).	
Other titles	▪ Cybersecurity Operations Manager (CSOC) ▪ Security Operations (SOC) Manager ▪ Cybersecurity Manager ▪ Information Systems Security Manager (Cybersecurity Operations)	
Related NOCs	0213 Computer and information systems managers	
Tasks	▪ Lead and manage SOC personnel including hiring, training, staff development, performance management and conducting annual performance reviews ▪ Maintain currency in cybersecurity threat landscape and security technologies ▪ Develop and implement an integrated SOC program that meets legislative and organizational requirements ▪ Develop and publish SOC governance mechanisms (policies, procedures and guidance) ▪ Develop and implement a measurement and quality assurance program ▪ Monitor and report on SOC program effectiveness to senior management ▪ Monitor and manage relationships with security services and technologies providers ▪ Provide strategic assessments on threat landscape, SOC technology trends, and emerging security technologies ▪ Seek and interpret threat intelligence based on organizational risks ▪ Manage cybersecurity events and incidents within the SOC ▪ Provide reports, briefings and risk-based recommendations on routine and non-routine cybersecurity events and incidents including responding to organizational crises (e.g. business systems shut-downs) ▪ Lead and facilitate lessons learned, post-mortem and best practices activities on cybersecurity events and incidents ▪ Develop and oversee implementation of action plans in support of continuous improvement of cybersecurity posture	
Required qualifications	Education	Bachelor's degree in computer science or related discipline or College diploma in IT field.
	Training	Cybersecurity operations training with industry-level certification in related field (e.g. network security, incident handling, threat detection and mitigation, digital forensics).

<table>
<tr><td></td><td></td><td>Security operations team management training or equivalent development and experience.
Training on organization relevant tools and technology that support cybersecurity operations</td></tr>
<tr><td></td><td>Work experience</td><td>Significant (5-10 years) experience in IT domain with 3-5 years' experience in cybersecurity operations or related domain.</td></tr>
<tr><td>Tools & Technology</td><td colspan="2">▪ Incident management processes and procedures
▪ Defensive systems including firewalls, anti-virus software and systems, intrusion detection and protection systems, scanners and alarms
▪ Security event and incident management systems and/or incident reporting systems and networks,
▪ Authentication software and systems,
▪ Vulnerability management processes and vulnerability assessment systems including penetration testing if used
▪ Security services provided if applicable</td></tr>
<tr><td>Competencies</td><td colspan="2">Underpinning this occupation are those competencies demonstrated for an activity manager as well as the Information Systems Security Manager within the NICE framework. Specifically, this work requires:

Basic level of application of the following KSAs:
☐ Preventative technical, operational and management controls available and organizational responsibilities for those controls

Advanced level of application of the following KSAs
☐ Organizational threats and vulnerabilities including:
o Cybersecurity threat landscape and adapting SOC processes to meet the evolving threat
o Vulnerability management requirements and the range of potential mitigations available when a vulnerability management protocol does not exist
☐ Defensive systems management including:
o Firewalls, anti-virus, intrusion detection and protection systems
o Required manual and automated settings
o Monitoring, testing and maintenance requirements
☐ Developing, implementing, and managing:
o Incident management processes and policies
o Incident management responsibilities
o Incident monitoring and reporting practices in accordance with legislative requirements and organizational policies
o Post-incident analyses and reports
o Organizational lessons learned in support of continuous improvement
☐ Supplier management (if IT or security services are outsourced):
o Roles and responsibilities of security controls of supplied services
o Roles and responsibilities of supplier in incident management and reporting
o Incident monitoring, assessment and reporting requirements during the lifecycle of the contract
o Organizational responsibilities in response to a compromise/breach on the part of the supplier
o Managing supplier communications and relations during a crisis
☐ Advising on security requirements, policies, plans and activities
☐ Drafting and providing briefings and reports to different audience levels (users, managers, executives)</td></tr>
</table>

	☐ Maintaining broader security situational awareness ☐ Self-awareness regarding knowledge, skills and abilities required to respond to business, threat and technical changes ☐ Continuous learning to support currency in knowledge of emerging threats, technological innovations in security, and the changing cybersecurity landscape.
Future Trends Affecting Key Competencies	▪ The increased reliance on virtualized and/or 'cloud-based' services will require knowledge of responsibilities of the services provider including their responsibilities for detecting, responding to and recovering from a cybersecurity incident. ▪ If practiced within the organization, there will be a requirement to fully understand the implications of 'bring your own device' (BYOD) policies. This means that regardless of the device capabilities, there will need to be an assessment of the risks posed to the organization, mitigations to account for potential compromise through a personal device, and what actions will be required by the SOC in the event of an incident. ▪ Increased use of automated tools, aided by artificial intelligence, will require understanding of how the tools will be integrated into the SOC including implementation of personnel and process changes. ▪ Increased use of automated tools by threat actors pose challenges for organizations that do not have complementary defensive tools. Accordingly, creative, locally relevant mitigation strategies will be required. This will require well-honed critical and abstract thinking abilities. ▪ Mechanisms to support the required level of trust and organizational risk will need to be in place to support monitoring and reporting of results from automated tools. Consequently, there will need to be increased understanding of organizational risks posed within the dynamic threat environment. ▪ The emergence and use of quantum technologies by threat actors will fundamentally change encryption security. Understanding quantum threat capabilities and knowledge and skills related to implementing a quantum safe strategy will be required.

Cybersecurity Operations Analyst

Note: This role includes the following:

Tier I Analyst - Cybersecurity Operations Analyst

Tier II Analyst - Malware specialist

Tier III Analyst - Threat hunter: management and active defence

NICE Framework Reference	Protect and Defend, Cyber Defence Analyst, PR-CDA-001
Functional Description	Front-line cybersecurity operations center operator responsible for monitoring and maintaining IT security devices and is often responsible for initial detection, incident response and mitigation
Consequence of error or risk	Error, neglect, outdated information, lack of attention to detail or poor judgment could result in catastrophic failure of organizational IT and data systems and associated implications to the organizational functions which rely on those systems.
Development pathway	This is a common entry-level job within the security operations centre (SOC). With additional training and experience there is potential for more technically or operationally focused roles in cybersecurity operations (e.g. vulnerability assessment & management, digital forensics, threat analytics and malware analysis) as well as management opportunities. Note that Tier II and Tier III roles may require more extensive training and education in addition to relevant experience. Often a computer science or computer engineering degree is a pre-requisite given the level of knowledge and skill required in more complex tasks. However, there are many that have progressed from cybersecurity analyst positions to advanced cybersecurity roles without a related degree.
Other titles	▪ SOC Operator ▪ Cybersecurity Operator ▪ Infrastructure Security Analyst ▪ Network Security Analyst ▪ Network Security Administrator ▪ Data security analyst
Related NOCs	2171 Information systems analysts and consultants 2147 Computer engineers (except software engineers and designers) 2173 Software engineers and designers
Tasks	▪ Identify and analyze technical threats to, and vulnerabilities of, networks ▪ Identify, contain, conduct initial mitigations and report system compromises ▪ Review, analyze, and/or apply internet security protocols, cryptographic algorithms, directory standards, networking protocols, network hardening, technical IT security controls, IT security tools and techniques, OS, intrusion detection/protection systems, firewalls, routers, multiplexers and switches, and wireless devices ▪ Analyze security data and provide alerts, advisories and reports ▪ Install, configure, integrate, adjust, operate, monitor performance, and detect faults on security devices and systems ▪ Conduct impact analysis for new software implementations, major configuration changes and patch management ▪ Develop proof-of-concept models and trials for IT security products and services ▪ Troubleshoot security products and incidents

<table>
<tr><td></td><td colspan="2">▪ Design/develop IT Security protocols
▪ Complete tasks related to authorization and authentication in physical and logical environments
▪ Develop options and solutions to meet the security-related project objectives
▪ Identify the security products and its configuration to meet security-related project objectives
▪ Implement and test configuration specifications
▪ Develop configuration and operational build books
▪ Review, develop and deliver relevant training material</td></tr>
<tr><td rowspan="3">Required qualifications</td><td>Education</td><td>College diploma in IT field with specialization in IT/cybersecurity, network security or similar.</td></tr>
<tr><td>Training</td><td>Cybersecurity operations training with industry-level certification in related field (e.g. security operations, network security, threat detection and mitigation, security appliance operations). More advanced training required for Tier II and III analysts.</td></tr>
<tr><td>Work experience</td><td>Initial experiential requirement is to have been successful working in an IT environment and technical team setting.</td></tr>
<tr><td>Tools & Technology</td><td colspan="2">▪ Incident management processes and procedures
▪ Defensive systems including firewalls, anti-virus software and systems, intrusion detection and protection systems, scanners and alarms
▪ Security event and incident management systems and/or incident reporting systems and networks</td></tr>
<tr><td>Competencies</td><td colspan="2">In larger SOCs there may be the opportunity to progress from Tier 1 to Tier 2 analyst. Tier 3 analysts are rare and almost exclusively employed in national security and military contexts. The required competencies for Tier 1 and 2 are provided below.

For Tier 1 - Cybersecurity Operations Analyst

The following KSA are applied at a basic level:
☐ Network security administration and management
☐ Network security architecture
☐ Hardware and firmware security
☐ Software defined security and application security
☐ Virtualization and Virtual Private Network (VPN) security
☐ Cloud-based security
☐ Wireless/mobile device security
☐ IT security zoning
☐ Encryption and cryptography including key management concepts and principles
☐ Vulnerability scanning and analysis
☐ Vulnerability management tools, processes and procedures
☐ Web application security
☐ Configuration and operational build books
☐ System acquisitions and projects
☐ Legal and ethical responsibilities associated with cybersecurity operations including conduct of investigations, privacy, and preservation of evidence
☐ Writing and briefing on technical matters (e.g. incident reports, technical reports, etc.) for managerial level understanding</td></tr>
</table>

	The following KSA are applied at an advanced level: ☐ Network security appliance concepts, operation and configuration (equipment specific based on role - network, server and desktop cyber defence systems and/or appliances) ☐ Types of intrusions and indicators of compromise (IoCs) ☐ Sources of threat information ☐ Common threat actor tactics, techniques, and procedures (TTPs) ☐ Incident management processes, responsibilities and authorities ☐ Intrusion detection and prevention methodologies, tools and systems ☐ Intrusion analysis and mitigation techniques ☐ Basic malware analysis **For Tier II Analyst - Malware specialist** The following KSA are applied at an advanced level. All of the above plus: ☐ Persistent and sophisticated threat TTPs ☐ Cyber defence tools, techniques and procedures ☐ Development and testing of network security appliances (including scripts and coding). ☐ Advanced malware analysis and reverse malware engineering ☐ Implementing advance security controls in response to advanced persistent threats ☐ Advanced incident response and recovery activities **For Tier III Analyst - Threat hunter: management and active defence** The following KSA are applied at an advanced level: ☐ Advanced threat management ☐ Advanced threat actor TTPs including specialization of persistent threat actors (e.g. nation state, organized crime) ☐ Interpreting/synthesizing classified / sensitive threat intelligence from multiple sources ☐ Legal and ethical responsibilities associated with active defence techniques ☐ Exploitation analysis ☐ Threat hunting and active defence frameworks ☐ Developing complex courses of action including risk assessment and mitigation plan ☐ Active defence tactics, tools and procedures including advanced threat countermeasures and counter-countermeasures ☐ Adversarial thinking ☐ Developing, testing and deploying technical tools within an active defence framework to protect organizational information and systems at risk
Future Trends Affecting Key Competencies	▪ The increased reliance on virtualized and/or ‘cloud-based’ services will require knowledge of responsibilities of the services provider including their responsibilities for detecting, responding to and recovering from a cybersecurity incident. ▪ If practiced within the organization, there will be a requirement to fully understand the implications of ‘bring your own device’ (BYOD) policies. This means that regardless of the device capabilities, there will need to be an assessment of the risks posed to the organization, mitigations to

	account for potential compromise through a personal device, and what actions will be required by the SOC in the event of an incident. ▪ Increased use of automated tools, aided by artificial intelligence, will require understanding of how the tools will be integrated into the SOC including implementation of personnel and process changes. ▪ Increased use of automated tools by threat actors pose challenges for organizations that do not have complementary defensive tools. Accordingly, creative, locally relevant mitigation strategies will be required. This will require well-honed critical and abstract thinking abilities. ▪ Mechanisms to support the required level of trust and organizational risk will need to be in place to support monitoring and reporting of results from automated tools. Consequently, there will need to be increased understanding of organizational risks posed and potential responses within the dynamic threat environment. ▪ The emergence and use of quantum technologies by threat actors will fundamentally change encryption security. This will require knowledge and skills related to implementing a quantum safe strategy as well as threat actor tools, techniques and protocols related to quantum computing attacks and how to defend against them.

Cybersecurity Incident Responder

OT incident responder

NICE Framework Reference	Protect and Defend, Cyber Defence Incident Responder, PR-CIR-001
Functional Description	Provides immediate and detailed response activities to mitigate or limit unauthorized cybersecurity threats and incidents within an organization. This includes planning and developing courses of action; prioritizing activities; and supporting recovery operations and post-incident analysis.
Consequence of error or risk	Error, neglect, outdated information, lack of attention to detail or poor judgment could result in catastrophic failure of organizational IT and data systems and associated implications to the organizational functions which rely on those systems.
Development pathway	This is a common entry-level job within the security operations centre (SOC). With additional training and experience there is potential for more technically or operationally focused roles in cybersecurity operations such as vulnerability assessment & management, digital forensics, threat analytics and malware analysis.) as well as management opportunities.
Other titles	▪ Cybersecurity incident responder ▪ Security Operations Centre - Incident handler ▪ Cybersecurity first responder ▪ Operational technology security incident responder
Related NOCs	2171 Information systems analysts and consultants 2147 Computer engineers (except software engineers and designers) 2173 Software engineers and designers
Tasks	These tasks apply equally to IT and OT systems. ▪ Perform real-time cyber defense incident handling tasks (e.g., forensic collections, intrusion correlation and tracking, threat analysis, and direct system remediation) ▪ Conduct security triage to identify and analyze cyber incidents and threats ▪ Actively monitor networks and systems for cyber incidents and threats ▪ Conduct risk analysis and security reviews of system logs to identify possible cyber threats ▪ Conduct analysis and review, and/or apply network scanners, vulnerability assessment tools, network protocols, internet security protocols, intrusion detection systems, firewalls, content checkers and endpoint software ▪ Collect and analyze data to identify cybersecurity flaws and vulnerabilities and make recommendations that enable prompt remediation ▪ Develop and prepare cyber defence incident analysis and reporting ▪ Define and maintain tool sets and procedures ▪ Develop, implement, and evaluate prevention and incident response plans and activities, and adapt to contain, mitigate or eradicate effects of cybersecurity incident ▪ Provide incident analysis support on response plans and activities ▪ Conduct research and development on cybersecurity incidents and mitigations ▪ Create a program development plan that includes security gap assessments, policies, procedures, playbooks, and training manuals ▪ Review, develop and deliver relevant training material

Required qualifications	Education	College diploma in IT field with specialization in IT/cybersecurity, network security or similar.
	Training	Cybersecurity operations training with industry-level certification in related field (e.g. security operations, network security, threat detection and mitigation, security appliance operations). Specialized training required for Operational Technology and related systems.
	Work experience	Initial experiential requirement is to have been successful working in an IT environment and technical team setting.
Tools & Technology	▪ Incident management processes and procedures ▪ Defensive systems including firewalls, anti-virus software and systems, intrusion detection and protection systems, scanners and alarms ▪ Security event and incident management systems and/or incident reporting systems and networks	
Competencies	**Cybersecurity Incident Responder** The following KSA are applied at a basic level: ☐ Network security administration and management ☐ Network security architecture ☐ Hardware and firmware security ☐ Software defined security and application security ☐ Virtualization and VPN security ☐ Cloud-based security ☐ Wireless/mobile device security ☐ IT security zoning ☐ Encryption and cryptography including key management concepts and principles ☐ Vulnerability scanning and analysis ☐ Vulnerability management tools, processes and procedures ☐ Web application security ☐ Configuration and operational build books ☐ System acquisitions and projects ☐ Legal and ethical responsibilities associated with cybersecurity operations including conduct of investigations, privacy, and preservation of evidence ☐ Writing and briefing on technical matters (e.g. incident reports, technical reports, etc.) for managerial level understanding ☐ Business continuity and disaster response basics The following KSA are applied at an advanced level: ☐ Network security appliance concepts, operation and configuration (equipment specific based on role - network, server and desktop cyber defence systems and/or appliances) ☐ Types of intrusions and indicators of compromise (IoCs) ☐ Sources of threat information ☐ Common threat actor tactics, techniques, and procedures (TTPs) ☐ Incident management processes, responsibilities and authorities ☐ Intrusion detection and prevention methodologies, tools and systems ☐ Intrusion analysis and mitigation techniques ☐ Basic malware analysis ☐ Cybersecurity investigations and evidence preservation	

	For Operational Technology Incident Responder In addition to the relevant KSAs above, the follow applied at the basic level: ☐ OT systems software and hardware, programmable logic controllers, and digital and analog relaying ☐ Threat and risk assessment to internet connected OT (including implications and assessment of IoT devices) ☐ Legal and compliance requirements including organizational responsibilities for workplace and public safety related to OT/ production ☐ Telemetry systems, data communications, data acquisition and process control ☐ Operating systems, networking, and communications systems concepts ☐ Electrical distribution networks, power system equipment, transformer station operation and electrical theory ☐ Database management systems and applications ☐ Measures or indicators of OT system performance, availability, capacity, or configuration problems ☐ Analysis tools and network protocols ☐ Diagnostic tools and fault identification techniques
Future Trends Affecting Key Competencies	▪ The increased reliance on virtualized and/or 'cloud-based' services will require knowledge of responsibilities of the services provider including their responsibilities for detecting, responding to and recovering from a cybersecurity incident. ▪ If practiced within the organization, there will be a requirement to fully understand the implications of 'bring your own device' (BYOD) policies. This means that regardless of the device capabilities, there will need to be an assessment of the risks posed to the organization, mitigations to account for potential compromise through a personal device, and what actions will be required by the SOC in the event of an incident. ▪ Increased use of automated tools, aided by artificial intelligence, will require understanding of how the tools will be integrated into the SOC including implementation of personnel and process changes. ▪ Increased use of automated tools by threat actors pose challenges for organizations that do not have complementary defensive tools. Accordingly, creative, locally relevant mitigation strategies will be required. This will require well-honed critical and abstract thinking abilities. ▪ Mechanisms to support the required level of trust and organizational risk will need to be in place to support monitoring and reporting of results from automated tools. Consequently, there will need to be increased understanding of organizational risks posed and potential responses within the dynamic threat environment. ▪ The emergence and use of quantum technologies by threat actors will fundamentally change encryption security. This will require knowledge and skills related to implementing a quantum safe strategy as well as threat actor tools, techniques and protocols related to quantum computing attacks and how to defend against them.

Cybersecurity Operations Technician

NICE Framework Reference	Protect and Defend, PR-INF-001, Cybersecurity Defence Infrastructure Support	
Functional Description	Tests, implements, deploys, maintains, and administers the security operations infrastructure hardware and software.	
Consequence of error or risk	Error, neglect, outdated information, lack of attention to detail or poor judgment could result in security system failure or system compromise which may have a significant impact on organizational IT systems, capabilities or functions.	
Development pathway	This is an often an entry-level job to the security domain after gained experience in technical, network administrative, or other similar functions. With additional training and experience there is potential for more technically or operationally focused roles as well as management opportunities.	
Other titles	▪ Security infrastructure support specialist/technician ▪ Security systems analyst ▪ Security systems technician ▪ Security control analyst	
Related NOCs	2171 Information systems analysts and consultants 2281 Computer network technicians 2282 User support technicians	
Tasks	▪ Actively monitor security system performance, troubleshoot and resolve hardware or software interoperability issues, and system outages and faults ▪ Install, configure, and maintain security system software, hardware, and peripheral equipment ▪ Develop, conduct, and maintain incident reports and vulnerability and impact assessments ▪ Develop and maintain tracking and solution database ▪ Analyze and recommend improvements and changes to support improved security operations ▪ Audit, log and report life-cycle management activities ▪ Administer security system accounts, privileges, and access to systems and equipment ▪ Conduct asset management or inventory control of system and equipment resources ▪ Develop, deliver, and oversee training material and educational efforts	
Required qualifications	Education	Post-secondary education (degree or diploma in related computer science or IT field
	Training	Training in cybersecurity systems, security systems operations and vendor-based tools (e.g. intrusion detection systems, firewalls, anti-virus, incident management, etc.)
	Work experience	2 – 3 years in network operations and security
Tools & Technology	▪ Cybersecurity systems tools, logs, and procedures ▪ Organizational policies and directives ▪ Security event and incident management systems and/or incident reporting systems and networks	

Competencies	KSAs applied at the basic level: ☐ Threats to information systems and their security ☐ Network security architecture concepts, protocols, components, and principles (e.g., application of defense-in-depth). ☐ Basic system, network, and OS hardening techniques. ☐ Transmission records and modes (e.g., Bluetooth, Radio Frequency Identification (RFID), Infrared Networking (IR), Wireless Fidelity (Wi-Fi). paging, cellular, satellite dishes, Voice over Internet Protocol (VoIP)) ☐ Network traffic analysis (tools, methodologies, processes) ☐ Identity, credential and access management architectures and standards ☐ Cybersecurity incident management policy, procedures and practices ☐ Organizational analysis of user and business trends ☐ Client consultation and problem resolution KSAs applied at an advanced level: ☐ Cybersecurity systems test procedures, principles, and methodologies ☐ Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) tools and applications ☐ Install, configure, operate, maintain and monitor related applications ☐ Cybersecurity infrastructure troubleshooting, analysis and remediation ☐ Cybersecurity systems policies, account management and controls
Future Trends Affecting Key Competencies	▪ The increased reliance on virtualized and/or 'cloud-based' services will require knowledge of responsibilities of the services provider including their responsibilities for cybersecurity systems management. ▪ If practiced within the organization, there will be a requirement to fully understand the implications of 'bring your own device' (BYOD) policies. This means that regardless of the device capabilities, there will need to be an assessment of the risks posed to the organization, mitigations to account for potential compromise through a personal device, and what actions will be required by the SOC in the event of an incident. ▪ Increased use of automated tools, aided by artificial intelligence, will require understanding of how the tools will be integrated into identity and access management processes and the related technical and process changes. ▪ Mechanisms to support the required level of trust and organizational risk will need to be in place to support monitoring and reporting of results from automated tools. Consequently, there will need to be increased understanding of organizational risks posed and potential responses within the dynamic threat environment. ▪ The emergence and use of quantum technologies by threat actors will fundamentally change encryption security. This will require knowledge and skills related to implementing a quantum safe strategy as well as threat actor tools, techniques and protocols related to quantum computing attacks and how to defend against them.

Vulnerability Assessment Analyst

NICE Framework Reference	Protect and Defend, PR-VAM-001, Vulnerability Assessment (VA) Analyst	
Functional Description	Scans applications and operating systems to identify flaws, and vulnerabilities; and conducts and presents vulnerability assessments on an organization's networks and systems.	
Consequence of error or risk	Error, neglect, outdated information, lack of attention to detail or poor judgment could result in mis-identifying or not detecting vulnerabilities which could be comprised. This may have a significant impact on organizational IT systems, capabilities or functions.	
Development pathway	This is often a tier 2 position within a cybersecurity operations environment that is normally preceded by 2-3 years in a network or operational security role. This can lead to increased specialization as a vulnerability analyst, red/blue team leader, penetration tester or management roles.	
Other titles	▪ Vulnerability tester ▪ Vulnerability assessor ▪ Vulnerability assessment manager	
Related NOCs	2171 Information systems analysts and consultants 2147 Computer engineers (except software engineers and designers) 2173 Software engineers and designers	
Tasks	▪ Identify critical flaws in applications and systems that cyber actors could exploit ▪ Conduct vulnerability assessments of relevant technology (e.g., computing environment, network and supporting infrastructure, and applications) ▪ Prepare and present comprehensive vulnerability assessments; ▪ Conduct network security audits and scanning ▪ Maintain deployable cyber defense audit toolkit (e.g., specialized cyber defense software and hardware) to support cyber defense operations ▪ Prepare audit reports that identify technical and procedural findings, and make recommendations on corrective strategies and solutions ▪ Conduct and/or support authorized penetration testing on organization networks and systems ▪ Define and review requirements for information security solutions ▪ Make recommendations on the selection of cost-effective security controls to mitigate risks ▪ Develop, deliver, and oversee training material and educational efforts	
Required qualifications	Education	Post-secondary education (degree or diploma) in related computer science or IT field.
	Training	Training in cybersecurity systems, vulnerability assessment and analysis. Vendor-based vulnerability system training.
	Work experience	2 – 3 years in a network or cybersecurity operations role.
Tools & Technology	▪ Organizational security policies, procedures and practices ▪ VA tools ▪ Vulnerability management policies, processes and practices	

	▪ Common vulnerability databases
Competencies	KSAs applied at the basic level: ☐ Advanced threat actor tools, techniques and protocols ☐ Penetration testing principles, tools, and techniques ☐ Risk management processes for assessing and mitigating risks ☐ System administration concepts ☐ Cryptography and cryptographic key management concepts ☐ Cryptology ☐ Identifying security issues based on the analysis of vulnerability and configuration data ☐ Vulnerability management policies, processes and practices KSAs applied at an advanced level: ☐ VA planning and scheduling including system risks and mitigations ☐ System and application security threats and vulnerabilities ☐ System administration, network, and operating system hardening techniques ☐ Packet analysis using appropriate tools ☐ Conducting vulnerability scans and recognizing vulnerabilities in security systems ☐ Conducting vulnerability/impact/risk assessments ☐ Reviewing system logs to identify evidence of past intrusions ☐ Using network analysis tools to identify vulnerabilities
Future Trends Affecting Key Competencies	▪ The increased reliance on virtualized and/or 'cloud-based' services will require knowledge of responsibilities of the services provider including their responsibilities for detecting, responding to and recovering from a cybersecurity incident. ▪ If practiced within the organization, there will be a requirement to fully understand the implications of 'bring your own device' (BYOD) policies. This means that regardless of the device capabilities, there will need to be an assessment of the risks posed to the organization, mitigations to account for potential compromise through a personal device, and what actions will be required by the SOC in the event of an incident. ▪ Increased use of automated tools, aided by artificial intelligence, will require understanding of how the tools will be integrated into the SOC including implementation of personnel and process changes. ▪ Increased use of automated tools by threat actors pose challenges for organizations that do not have complementary defensive tools. Accordingly, creative, locally relevant mitigation strategies will be required. This will require well-honed critical and abstract thinking abilities. ▪ Mechanisms to support the required level of trust and organizational risk will need to be in place to support monitoring and reporting of results from automated tools. Consequently, there will need to be increased understanding of organizational risks posed and potential responses within the dynamic threat environment. ▪ The emergence and use of quantum technologies by threat actors will fundamentally change encryption security. This will require knowledge and skills related to implementing a quantum safe strategy, understanding system vulnerabilities and how to mitigate quantum-related threats.

Penetration Tester

NICE Framework Reference	None.	
Functional Description	Conducts formal, controlled tests and physical security assessments on web-based applications, networks, and other systems as required to identify and exploit security vulnerabilities.	
Consequence of error or risk	Error, neglect, outdated information, lack of attention to detail or poor judgment could result in mis-identifying or not detecting vulnerabilities which could be comprised. This may have a significant impact on organizational IT systems, capabilities or functions.	
Development pathway	This is often a tier 2 / 3 position within a cybersecurity operations environment that is normally preceded by significant experience (3-5 years) in a cybersecurity operations role including employment within Vulnerability Analysis, Malware Analysis or Technical Analysis of security systems. This is an advanced technical role, which can lead to increasing technical specialization, red team leadership or management roles.	
Other titles	▪ Security Testing and Evaluation Specialist ▪ Advanced Vulnerability Assessment Analyst	
Related NOCs	2171 Information systems analysts and consultants 2147 Computer engineers (except software engineers and designers) 2173 Software engineers and designers	
Tasks	▪ Complete penetration tests on web-based applications, network connections, and computer systems to identify cyber threats and technical vulnerabilities ▪ Conduct physical security assessments of an organization's network, devices, servers, and systems ▪ Develop penetration tests and the tools needed to execute them (e.g. standards, risks, mitigations) ▪ Investigate for unknown security vulnerabilities and weaknesses in web applications, networks, and relevant systems that cyber actors can easily exploit ▪ Develop and maintain documents on the results of executed pen testing activities ▪ Employ social engineering to uncover security gaps ▪ Define and review requirements for information security solutions ▪ Analyze, document, and discuss security findings with management and technical staff ▪ Provide recommendations and guidelines on how to improve upon an organization's security practices ▪ Develop, deliver, and oversee training material and educational efforts	
Required qualifications	Education	Post-secondary education (degree or diploma in related computer science or IT field).
	Training	Training in vulnerability analysis and penetration testing tools, techniques and procedures.
	Work experience	2-3 years' experience in an advanced cybersecurity operations role, preferably with VA experience.
Tools & Technology	▪ Organizational security policies, procedures and practices ▪ Organizational systems map and network architecture	

	▪ VA tools ▪ Vulnerability management policies, processes and practices ▪ Common vulnerability databases ▪ Penetration testing tools and protocols
Competencies	KSAs applied at an advanced level: ☐ Network security architecture ☐ Advanced threat actor tools, techniques and protocols ☐ Penetration testing principles, tools, and techniques ☐ Risk management processes for assessing and mitigating risks ☐ System administration concepts ☐ Cryptography and cryptographic key management concepts ☐ Cryptology ☐ Identifying security issues based on the analysis of vulnerability and configuration data ☐ Vulnerability management policies, processes and practices ☐ Penetration test planning and scheduling including system risks and mitigations ☐ System and application security threats and vulnerabilities ☐ System administration, network, and operating system hardening techniques ☐ Packet analysis using appropriate tools ☐ Conducting vulnerability scans and recognizing vulnerabilities in security systems ☐ Conducting vulnerability/impact/risk assessments ☐ Reviewing system logs to identify evidence of past intrusions ☐ Using network analysis tools to identify vulnerabilities
Future Trends Affecting Key Competencies	▪ The increased reliance on virtualized and/or 'cloud-based' services will require knowledge of responsibilities of the services provider including their responsibilities for detecting, responding to and recovering from a cybersecurity incident. ▪ If practiced within the organization, there will be a requirement to fully understand the implications of 'bring your own device' (BYOD) policies. This means that regardless of the device capabilities, there will need to be an assessment of the risks posed to the organization, mitigations to account for potential compromise through a personal device, and what actions will be required by the SOC in the event of an incident. ▪ Increased use of automated tools, aided by artificial intelligence, will require understanding of how the tools will be integrated into the SOC including implementation of personnel and process changes. ▪ Increased use of automated tools by threat actors pose challenges for organizations that do not have complementary defensive tools. Accordingly, creative, locally relevant mitigation strategies will be required. This will require well-honed critical and abstract thinking abilities. ▪ Mechanisms to support the required level of trust and organizational risk will need to be in place to support monitoring and reporting of results from automated tools. Consequently, there will need to be increased understanding of organizational risks posed and potential responses within the dynamic threat environment. ▪ The emergence and use of quantum technologies by threat actors will fundamentally change encryption security. This will require knowledge and skills related to implementing a quantum safe

	strategy, understanding system vulnerabilities and how to mitigate quantum-related threats.

Digital Forensics Analyst

NICE Framework Reference	Investigate, Cyber Defence Forensic Analyst, INV-FOR-002
Functional Description	**The following role-based description is for security operations only and does not include criminal or audit forensics functions which are provided for within the related law enforcement or audit related occupations**. Conducts digital forensics to analyze evidence from computers, networks, and other data storage devices. This includes investigating and preserving electronic evidence; planning and developing tools; prioritizing activities; and supporting recovery operations and post-incident analysis.
Consequence of error or risk	Error, neglect, outdated information, lack of attention to detail or poor judgment could result in a failure to determine the source and mitigate a compromise, but additionally may result in impacts to organizational information systems to include criminal charges or civil litigation.
Development pathway	This is often a tier 2/3 position within a cybersecurity operations environment that is normally preceded by a minimum of 2-3 years in a network or operational security role including as a malware analyst. This can lead to increased specialization within digital forensics or security assessment activities as well as red/blue team leader, penetration tester or management roles.
Other titles	▪ Digital forensics investigator (normally reserved for cybercrime environment) ▪ Digital forensics examiner (normally reserved for cyber audit environments)
Related NOCs	2171 Information systems analysts and consultants 2147 Computer engineers (except software engineers and designers) 2173 Software engineers and designers
Tasks	▪ Perform real-time cyber defence incident investigations (e.g., forensic collections, intrusion correlation and tracking, and threat analysis) ▪ Investigate security incidents as per terms of reference ▪ Plan forensics analysis activities for cyber incidents ▪ Collect and analyze intrusion artifacts (e.g., source code, malware, and system configuration) and use discovered data to enable mitigation of potential cyber defense incidents ▪ Identify and accurately report on digital forensic analysis artifacts ▪ Capture and analyze network traffic associated with malicious activities using network monitoring tools ▪ Contribute to post-analysis on security incidents and make recommendations based on forensics activities ▪ Develop and maintain investigative and technical reports ▪ Provide technical assistance on digital evidence matters to appropriate personnel ▪ Compile evidence for legal cases, and provide expert testimony at court proceedings ▪ Manage digital evidence in accordance with appropriate chain of custody requirements ▪ Identify and manage secure analysis infrastructure/laboratory

<table>
<tr><td></td><td colspan="2">▪ Operate digital forensics systems (as required based on function and systems available)
▪ Prepare and review forensics policies, standards, procedures and guidelines
▪ Develop, deliver, and oversee training material and educational efforts</td></tr>
<tr><td rowspan="3">Required qualifications</td><td>Education</td><td>Post-secondary education (degree or diploma in related computer science or IT field).</td></tr>
<tr><td>Training</td><td>Training in digital forensics tools, techniques and procedures. Also, depending on the organizational technical context and systems/devices used, specialized digital forensics training may be required (e.g. mobile device, digital media, etc.)</td></tr>
<tr><td>Work experience</td><td>2-3 years’ experience in an advanced cybersecurity operations role, preferably with malware analysis experience in ‘dead box’ and active environments.</td></tr>
<tr><td>Tools & Technology</td><td colspan="2">▪ Organizational security policies, procedures and practices
▪ Organizational systems map and network architecture
▪ Digital forensics tools, techniques and procedures
▪ Malware analysis tools
▪ Security Event and Incident Management System
▪ Common vulnerability databases
▪ Security investigation terms of references, responsibilities and limits of authority</td></tr>
<tr><td>Competencies</td><td colspan="2">KSAs applied at an advanced level:
☐ Threat actor tools, techniques and procedures
☐ Incident response and handling methodologies
☐ Security Event and Incident Management System
☐ Digital forensics methodologies, processes and practices
☐ Anti-forensics tactics, techniques, and procedure
☐ Processes for collecting, packaging, transporting, and storing electronic evidence to avoid alteration, loss, physical damage, or destruction of data
☐ Seizing and preserving digital evidence
☐ Applicable laws, regulations, policies and ethics as they relate to investigations and governance
☐ Legal rules of evidence and court procedures, presentation of digital evidence, testimony as an expert witness
☐ System or device specific forensics (e.g. memory, active director, mobile device, network, computer (dead box), etc.)
☐ Malware analysis tools and techniques
☐ Reverse engineering
☐ Deployable digital forensics capabilities
☐ Types of digital forensics including tools, techniques and procedures (organization and information system dependent) which may include the following forensics for:
○ computer
○ network and active directory;
○ mobile devices
○ digital media (image, video, audio)
○ memory</td></tr>
</table>

Future Trends Affecting Key Competencies	▪ The increased reliance on virtualized and/or 'cloud-based' services will require knowledge of responsibilities of the services provider including their responsibilities for cybersecurity systems management. ▪ If practiced within the organization, there will be a requirement to fully understand the implications of 'bring your own device' (BYOD) policies. This means that regardless of the device capabilities, there will need to be an assessment of the risks posed to the organization, mitigations to account for potential compromise through a personal device, and what actions will be required by the SOC in the event of an incident. ▪ Increased use of automated tools, aided by artificial intelligence, will require understanding of how the tools will be integrated into identity and access management processes and the related technical and process changes. ▪ Mechanisms to support the required level of trust and organizational risk will need to be in place to support monitoring and reporting of results from automated tools. Consequently, there will need to be increased understanding of organizational risks posed and potential responses within the dynamic threat environment. ▪ The emergence and use of quantum technologies by threat actors will fundamentally change encryption security. This will require knowledge and skills related to implementing a quantum safe strategy as well as threat actor tools, techniques and protocols related to quantum computing attacks and how to defend against them.

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)

Annex D - The Cybersecurity Generalist

Within many small and medium organizations (SMOs), and even within larger organizations that are not heavily reliant on internet-based activities, there are individuals tasked with cybersecurity responsibilities who may not have any IT or cybersecurity background. While not specifically the province of the NOS, this annex provides a more detailed description of cybersecurity competencies that can serve as a reference to employers, educators and workforce development professionals seeking a better understanding of the requirements of this role.

Applicable job titles: Corporate Security Officer, Security Analyst, Security Officer, Security Manager, etc.

Cybersecurity Generalists:

- Perform cybersecurity functions on a part-time basis in conjunction with other responsibilities;
- Only require cybersecurity knowledge, skills and abilities commensurate with their business, technical and threat context; and
- Are not considered cybersecurity professionals and do not have a cybersecurity career trajectory.

Common tasks include:

- Assess the organization’s cybersecurity posture
- Facilitate identification of organizational cyber risks
- Identify non-technical cybersecurity controls
- Identify and liaise with technical experts, internal or external, on technical controls
- Develop organizational cybersecurity plans and policies
- Advise leadership on security awareness and training
- Monitor and support technical experts, whether in-house or out-sourced, in their cybersecurity functions
- Coordinate cybersecurity incident response
- Monitor and report on response and mitigation actions and recommend courses of action based on technical advice
- Coordinate post-mortem activities on events and incidents, integrating lessons learned into organizational policies and procedures

For many of these tasks, there are ample online resources available to guide the security generalists in their duties. Underpinning effectiveness in these tasks, however,

are basic knowledge, skills and abilities (KSAs) needed to support decision making and action. However, it is unlikely that they will have any extensive cybersecurity training or education. Accordingly, they should be offered sufficient learning opportunities to attain the required competencies commensurate with their responsibilities as well as the threat, technical and business context. As shown in the examples in the figure below, this typically requires competencies borrowed from some of the work roles within each major work category.

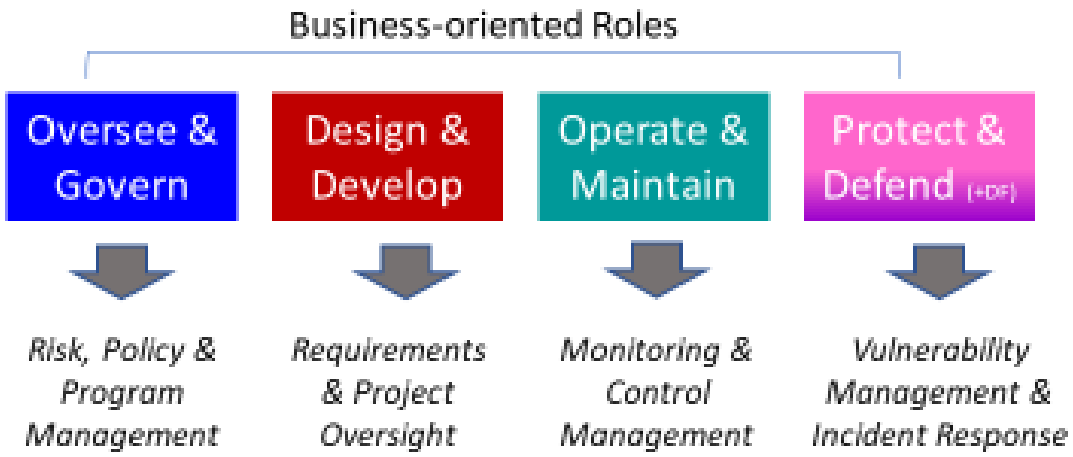

Figure – Cybersecurity generalist functions drawn from existing activity areas

Basic Knowledge:

- Technical context (e.g. organizational IT infrastructure, software, devices and policies)
- Cyber threat context (including deliberate, accidental, natural hazards)
- Business context (priorities, objectives, market, trends)
- Legal, policy and ethical context for security
- Cybersecurity risk management as part of organizational risk
- Cybersecurity incident management (domain specific)
- Cybersecurity processes, technology, trends and emerging issues
- Sources of cybersecurity expertise and resources

Basic Skills and Abilities:

- Providing business advice within the legal & policy cybersecurity context

- Exercising foresight and security planning to support digital business activities and growth
- Translating cyber risk to corporate risk
- Differentiating between compliance and risk
- Interpreting threat and risk assessments for the business context
- Assessing effectiveness of security controls against organizational security objectives

Annex E – Acronym List

ICT	Information, Communication and Technology
BCP	Business Continuity Plan
BYOD	Bring your own device
CIO	Chief Information Officer
COMSEC	Communications Security
CSOC	Cybersecurity Operations Manager
CTA	Cybersecurity Talent Alliance
CWF	Cybersecurity Workforce Framework (US)
DC	Digital Certificate
DCS	Distributed Control System
DRP	Disaster Response Plan
HSM	Hardware Security Module
ICAM	Identity, Credentials and Access Management
ICS	Industrial control system
IDS	Intrusion Detection System
IoC	Indicators of Compromise
IPS	Intrusion Prevention System
IR	Infrared Networking
IT	Information Technology
KSA	Knowledge, Skills and Abilities
NICE	National Initiative on Cybersecurity Education (US)
NOC	National Occupation Classification
NIST	National Institute of Standards and Technology (US)
OCS	Operational Control Systems
OS	Operating System
OT	Operations Technology
PKI	Public Key Infrastructure
RFID	Radio Frequency Identification
SCADA	Supervisory control and data acquisition
SOC	Security Operations Centre
SSH	Secure Shell
SSL	Secure Socket Layer
TLS	Transport Layer Security
TTPs	Tactics, Techniques and Procedures
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
Wi-Fi	Wireless Fidelity