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Consequence of error or risk	Error, neglect, outdated information or failure to account for organizational requirements, business needs and threats could result in poor systems design and/or integration of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.