

Good day, as per the request for comments dated 19 Nov 2019, I have included the attached observations on the NICE Cybersecurity Workforce Framework from the Information Technology Association of Canada (ITAC). Please note that these comments are based on ITAC's research and work and do not necessarily express the opinions or perspectives of the Government of Canada.

Questions or clarifications on the observations can be directed to the undersigned.

Thank you for the opportunity to provide comments.

Randy

Randy Purse, CD, PhD, CTD
Director, Cybersecurity Standards, ITAC Talent
ITAC | Information Technology Association of Canada

www.itactalent.ca/

<https://itactalent.ca/our-programs/cta/>

13 January 2019

NICE – Request for Comments

Reference: NIST Seeking Input on Updates to NICE Cybersecurity Workforce Framework, 19 November 2019, <https://www.nist.gov/news-events/news/2019/11/nist-seeking-input-updates-nice-cybersecurity-workforce-framework>

Aim. This document provides input to the comprehensive review of the National Initiative on Cybersecurity Education, Cybersecurity Workforce Framework (the NICE Framework) as requested at reference.

Background. The Information Technology Association of Canada (ITAC) has been working with Employment and Skills Development Canada (ESDC) of the Government of Canada on a project to develop and deliver several products and services intended to support cybersecurity skills development in Canada. This work includes the development of a Canadian cybersecurity skills framework based upon elements of the NICE framework and a National Occupational Specification (NOS) for cybersecurity. The information gathered from ITAC's research within the Canadian cybersecurity community forms the basis of the comments that follow.

While a more formal report to the Canadian government is in the final stages, ITAC is submitting its observations and recommendations now to support the NICE Framework review. Accordingly, please note that while the comments are based on ITAC's work on the Canadian cybersecurity skills framework, they do not necessarily reflect the opinions or perspectives of the Government of Canada.

Key Observations and Recommendations. The following key observations and recommendations are forwarded for consideration in the upcoming NICE revision.

First, there are several positive attributes of the NICE framework. It is a comprehensive and detailed account of cybersecurity work which also:

- is readily available to the Canadian labour market and workforce development stakeholders;
- standardizes cybersecurity work role descriptions and provides a common lexicon for the community within the U.S. and Canada as well as other nations;
- provides a detailed description of knowledge, skills and abilities (KSAs) for common cybersecurity roles, and recently introduced associated competencies that will aid in training, education and career development;
- creates a known base-line to assess skilled entry candidates;
- is internationally supported; and
- supports worker portability nationally and internationally.

However, based on ITAC's research and engagement with the broader business community, there are three key areas for improvement that should be considered during the upcoming review:

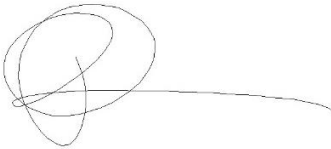
1. **Aligning the NICE Framework with industry/business community taxonomy & organizational structures.** As the NICE Framework was largely developed for the U.S. Fed Gov, it includes terms and a structure that do not translate well to those used within industry and is typically too large and complex for most businesses and industries, in particular small and medium enterprises (SMEs). Accordingly, it is recommended that in the upcoming revision, the NICE Framework:
 - a. provide representations that can scale to small/medium enterprises or organizations that are less tech enabled. This includes explicit identification of roles common within organizational security and how the NICE Framework can be interpreted to support such roles. This can also include the role of a 'cybersecurity generalist' which is common to organizations who do not employ cybersecurity specialists, but nonetheless require enough understanding of the business, technical and threat context to be able to liaise with third-party technology and security services and product providers (e.g. such as Corporate Security Officers);
 - b. change the name of the work category "securely provision" be aligned with business/industry taxonomy that represents the majority of specialisations and work roles – 'Design and Develop';
 - c. more clearly distinguish between core cybersecurity work roles (explicit security roles) and those that are in cybersecurity hybrid or adjacent roles that have some security functions, but are not primarily employed in cybersecurity (e.g. many of the Oversee & Govern, Securely Provision, Operate & Maintain work roles); and
 - d. de-emphasizes or more clearly distinguishes between typical organizational cybersecurity functions and those within the national security / international security domain (e.g. advanced operator, analyst, and intelligence functions) which tend to be highly specialized and follow a more well-defined career path whether within Fed Gov or private sector organizations.
2. **Representing example cybersecurity career pathways.** The NICE Framework presents cybersecurity work in a static way which may lead to the impression that all work is stable within a specific role and that there is limited career growth within a role or within cybersecurity writ large. While there are other representations available (e.g. cyberseek.org), as the defining document, the NICE Framework should explicitly include representations of potential career paths to remove possible misconceptions around cybersecurity work to include examples of:
 - a. Increasing levels of technical expertise within a work role (e.g. potential growth from Tier 1 to Tier three cybersecurity operations analyst); and

- b. Growth within or across work categories (e.g. moving from a junior technical to a senior technical role or moving from a predominantly technical work category to increasing responsibility in an advisory or management role in *Oversee & Govern*).

3. Ensuring that the NICE Framework represents emerging work and the evolution of the cybersecurity field. The original NICE Framework structure was created over a decade ago and, given both technological changes and our changing appreciation of the cybersecurity work there are additional or new work roles that should be included in the NICE. Several new / additional work roles have been identified within the Canadian context which have been included in the appendix. This includes introduction of cryptography and operational technology roles.

Conclusion. The NICE Framework is providing a strong foundation upon which to build a Canadian national cybersecurity skills framework. As noted, there are a few key areas that would, in ITAC's view, better address the needs of business and industry external to the federal government.

In closing, thank you for the opportunity to provide input to the upcoming NICE Framework revision. Any questions or clarifications regarding the above can be directed to the undersigned.



Randy Purse, CD, PhD, CTDP
Director, Cybersecurity Standards
Information Technology Association of Canada

Appendix 1 – Suggested Work Roles for Consideration in the NICE Framework

APPENDIX 1 – SUGGESTED WORK ROLES FOR CONSIDERATION IN THE NICE FRAMEWORK

The following table draws upon the existing NICE Framework and represents common cybersecurity work roles within the larger corporate/industrial context using the Canadian framework. Additional work roles within the Canadian workforce have been identified and are included as noted. As well, core roles are distinguished from adjacent or hybrid roles.

Legend:

Existing NICE Role
Suggested NEW Role within the Canadian Framework

* Canadian Forces NOCs have not been included in this table as they are generally applicable to all roles.

Canadian Framework	Related NICE Work Category / Speciality Area	Roles	Comments
Oversee & Govern	Oversee & Govern		
Organizational Leadership & Risk			
	Executive Cyber Leadership (EXL)	Executive Cyber Leadership	Based on description this equates to CISO role
		Corporate Security Officer (CSO)	New role – supports organizations that do not have CIO/CISO. This is also representative of the ‘cybersecurity generalist’
		Chief Information Officer/Chief Technical Officer/ Chief Resiliency Officer	New role – targeted adjacent security roles that have direct cyber responsibilities
		Chief Risk Officer	New Role – emerging within the Canadian labour market
		C-Suite & Board members	New role – generic executive level roles that are the primary risk

Canadian Framework	Related NICE Work Category / Speciality Area	Roles	Comments
			owners within a business.
	Risk (RSK)	Authorizer	Often the COO, CIO or equivalent
		Risk Analyst	New role – all hazards risk, organizational risks and related cyber risks
Legal and Privacy Advice	Legal Advice and Advocacy (LGA)	Cyber Legal Advisor	
		Privacy Officer/Privacy Compliance Manager	
Training, Education and Awareness	Training, Education, and Awareness (TEA)	Cyber Instructional Curriculum Developer	
		Cyber Instructor	
		College/University Professor	New role to support PSE requirements – often discipline or specialty based
		Learning and Development Specialist	New role - to complement organizational learning structures that do not have cyber instructional staff (e.g. for security awareness, training and education)
Cybersecurity Management	Cybersecurity Management (MGT)	Information Systems Security Manager	
		Security Auditor	New role – in support of internal security audits
		Information Systems Security Officer (Generic work role)	New role – recognizes the requirement for large enterprises and need for security monitoring and management of specific or diverse systems

Canadian Framework	Related NICE Work Category / Speciality Area	Roles	Comments
		Communications Security (COMSEC) Manager	
Strategic Planning and Policy (SPP)	Strategic Planning and Policy (SPP)	Cyber Workforce Developer and Manager	Uncommon role within Canadian labour market
		Cyber Policy and Strategy Planner	
		Business Continuity/ Resiliency Planner	New role – supports BCP, emergency management and disaster recovery activity
Program/Project Management and Acquisition (PMA)	Program/Project Management and Acquisition (PMA)	Program Manager	
		IT Project Manager	
		Product Support Manager	
		IT Investment/Portfolio Manager	
		IT Program Auditor	
		Business Process Automation (RPA also) Analyst	New role – recognizes emerging field
		Procurement Specialist	New Role – acquisition of secure products or services as well as security services and products
		Supply Chain Integrity Analyst	New role – specialized analyst associated with supply chain and third-party threats
	Communications	Communications Specialist	New speciality and role – relevant for crisis management and incident response

Canadian Framework	Related NICE Work Category / Speciality Area	Roles	Comments
		Webmaster/Online Communications Manager	New role – relevant to most Internet enabled organizations in digital economy – monitoring of web apps and web performance.
		Data security advisor/Breach coach	New role – specialized, often legal, advisor on organization activities associated with event/incident management
Design & Develop	Securely Provision		
Risk Management (RSK)	Risk Management (RSK)	Security Control Assessor	
Software Development (DEV)	Software Development (DEV)	Software Developer	
		Secure Software Assessor	
Systems Architecture (ARC)	Systems Architecture (ARC)	Enterprise Architect	
		IT/systems Architect	New role – subordinate role to enterprise architect or for smaller infrastructures.
		Security Architect	
		Security Engineer / Technologist	New role – supports requirements definition and build of secure systems. This includes potential specialization in OT, ICS, SCADA systems
		Encryption Engineer/Technologist	New role – increasing importance emerging in quantum safe/resistant systems
		Cryptanalyst / Cryptographer	New role – highly specialized role

Canadian Framework	Related NICE Work Category / Speciality Area	Roles	Comments
			supporting existing and new cryptographic activities
		Security Automation Engineer/Technologist	New role – specializes in SOAR and RPA type activities
Technology R&D (TRD)	Technology R&D (TRD)	Research & Development Specialist	
Systems Requirements Planning (SRP)	Systems Requirements Planning (SRP)	Systems Requirements Planner	
		Business Analyst	New role – key role in defining system requirements in support of business activities
		Operational Technology Systems Security Analyst	New role – recognizes IoT and cyber specialization in OT, ICS, SCADA systems
		Security automation analyst	New role – supplements planning for security automation and integration
		Systems security analyst	
		Systems security planner	
Test and Evaluation (TST)	Test and Evaluation (TST)	System Testing and Evaluation Specialist	
Systems Development (SYS)	Systems Development (SYS)	Information Systems Security Developer	
		Systems Developer	
Operate & Maintain	Operate & Maintain		
Data Administration (DTA)	Data Administration (DTA)	Database Administrator	
		Data Analyst	

Canadian Framework	Related NICE Work Category / Speciality Area	Roles	Comments
		Data Privacy Specialist	New role – specialization in data privacy issues particularly related to international data exchange and storage and compromise
Data and Information Systems Management	Knowledge Management (KMG)	Knowledge Manager	
		Information Systems Manager	
		Data manager	
		Data security specialist	
	Customer Service and Technical Support (STS)	Technical Support Specialist	
	Network Services (NET)	Network Operations Specialist	
		Network security analyst	New role – primarily involved in monitoring and managing perimeter security.
	Systems Administration (ADM)	System Administrator	
	Identity, Credentials, Authentication, and Encryption	Encryption/Public Key Infrastructure Support	New role – maintenance and support for encryption/PKI
		Identity and authentication management support	New role – specialization in ID, authentication access and privilege management controls
	Systems Analysis (ANA)	Systems Security Analyst	
Protect & Defend	Protect & Defend		
	Cybersecurity Management (MGT)	Information Systems Security Manager –	New role – specialized management role to support cybersecurity

Canadian Framework	Related NICE Work Category / Speciality Area	Roles	Comments
		Cybersecurity Operations	operations and SOC/IR team development
	Cybersecurity Defense Analysis (CDA)	Cyber Defense Analyst	Equates to security operations centre analyst
		Operational Technology Cyber Defence Analyst	New role – analysis and IR support for security of OT, ICS, SCADA systems
	Cybersecurity Defense Infrastructure Support (INF)	Cyber Defense Infrastructure Support Specialist	
	Incident Response (CIR)	Cyber Defense Incident Responder	
	Vulnerability Assessment and Management (VAM)	Vulnerability Assessment Analyst	
		Penetration Tester	
		VAM manager	
	Digital Forensics	Cyber Defence Digital Forensics analyst	
Investigate	Investigate		
	Cyber Investigation (INV)	Cyber Crime Investigator	
	Digital Forensics (FOR)	Law Enforcement / Counter-Intelligence Forensics Analyst	
		Cyber Defense Forensics Analyst	
Collect & Operate	Refer to NICE Framework	As per NICE roles	
Analyze	Refer to NICE Framework	As per NICE roles	