

# National CIO Subcommittee on Information Protection

State of FPT Cybersecurity

PSCIOC CONFERENCE – SEPTEMBER 2022



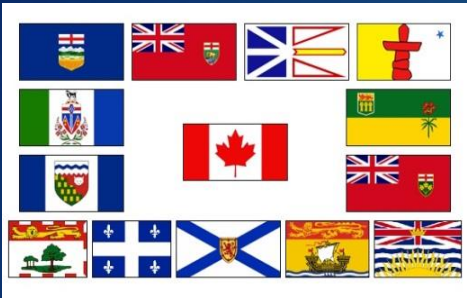
# AGENDA

- ▶ Reminder: NCSIP Charter – Highlights
- ▶ FPT Jurisdictions – Cybersecurity Capabilities Matrix
- ▶ Main Topics:
  - ▶ Overview of Current Cyber Threats to FPT
  - ▶ Major Common FPT Cybersecurity Activities
  - ▶ Proposal: Attraction and Retention of Cybersecurity Personnel
  - ▶ Discussion: NCSIP Reporting Relationship to PSCIOC



# Reminder: NCSIP Terms of Reference - Highlights

- ▶ Established in 1998 under PSCIOC
- ▶ Purpose:
  - ▶ To exchange information, actionable intelligence, policies, security awareness program practices and architecture initiatives related to information protection.
- ▶ Objectives:
  - ▶ To **enable secure digital government** through the exchange and leveraging of information and actionable intelligence, sharing of best practices, and joint solution research and development
  - ▶ To **improve the readiness of the Canadian public sector** to improve maturity of Canadian public sector security practices
  - ▶ **Ensure cybersecurity is championed** in Canadian public services
- ▶ Monthly video meetings and bi-annual “live” meetings, with adhoc meetings as required to focus on issues and special events



# FPT Cybersecurity Capabilities Matrix

(Not Up-To-Date – this version: August 2021)

	NL	NS	NB	PEI	QC	ON	MB	SK	AB	BC	YT	NT	NU	ATL	East	Prai	West
Responsibility for cyber security clearly assigned	In	In	In	In	In	In	In	In	In	In	In	In	In		In	In	In
Enterprise Cyber Security Team - Number of Staff	4	24	9	3	32	65	5	8	43	51		4			4	1.25	1.5
Additional Cyber Security Staff across Organization	2	1	7	0	28	30	1	0	0	26		0			0	0.5	0
<b>TOTAL Cyber Security Staff within Jurisdiction</b>	<b>6</b>	<b>25</b>	<b>16</b>	<b>3</b>	<b>60</b>	<b>95</b>	<b>6</b>	<b>8</b>	<b>43</b>	<b>77</b>	<b>0</b>	<b>4</b>	<b>0</b>	<b>0</b>	<b>4</b>	<b>1.75</b>	<b>1.5</b>
Supported Stakeholders per Cyber Security Staff	1,417	2,400	2,813	2,667	8,500	789	3,000	1,500	744	416		1,375			1,250	1,143	1,067
<b>THREAT IDENTIFICATION &amp; ASSESSMENT SERVICES</b>																	
Security Threat & Risk Assessment	In/Out	In/Out	In/Out	In/Out	In/Out	In	In	In	In	In/Out		In/Out				Out	In/Out
Security Threat & Risk Tracking/Management	In/Out	In/Out	In	In/Out	In/Out	In	In	In	In	In		In				In	In
Vulnerability Scanning - Infrastructure based	In/Out	In/Out	In	In	In/Out	In	In	In	In	In		In			In	Out	In
Vulnerability Scanning - Application based	In/Out	In/Out	In	In/Out	In/Out	In/Out	In	In	Out	In/Out		Out				Out	In
Vulnerability Management and Reporting	In	In	In	In	In/Out	In	In	In	In	In		Out			In	Out	In
Cyber Threat Intelligence Research	In/Out	In/Out	In	In/Out	In/Out	In	In/Out	Out	In	In/Out		Out				In/Out	In/Out
Cyber Threat Intelligence Reporting	In	In/Out	In	In	Out	In		In	In	In/Out		In/Out				In/Out	In/Out
<b>PROTECTION &amp; DETECTION SERVICES</b>																	
Security Operations Centre Services		In/Out	In	Out	In/Out	In	In/Out	In	Out	In		Out			In	Out	
Firewall Management	In	In	In	In	In/Out	In/Out	In/Out	In	Out	In		In			In	In	In
End Point Management - Servers	In	In	In	In	In/Out	In/Out	Out	In	In	Out		In			In	In	In
End Point Management - Desktops	In	In	In	In	In/Out	In/Out	Out	In	In	Out		In			In	In	In
End Point Management - Mobile Devices	In	In	In	In	In/Out	In/Out	Out	In	In	Out		In			In	In	In
Antivirus Management - Servers	In	In	In	In	In/Out	In	Out	In	In	Out		In			In	In	In
Antivirus Management - Desktops	In	In	In	In	In/Out	In	Out	In	Out	Out		In			In	In	In
Antivirus Management - Mobile Devices	In	In	In	In	In/Out	In	Out	Out	In	Out		In			In	In	In
Network Traffic Monitoring	In	In	In	In/Out	In/Out	In	In/Out	In	Out	In		In			In	In / Out	In
Host Log Monitoring	In	In/Out	In	In/Out	In/Out	In	In/Out	Out	Out	In/Out		In				In/Out	In
Security Information Event Monitoring (SIEM)	In	In	In	In/Out	In/Out	In	In/Out	In	In/Out	In/Out		Out				In/Out	In
Cloud Services Access Monitoring	In	In/Out	In	In	In/Out	In/Out		Out	In						In	In/Out	In
Implementation & Configuration of Security Controls	In	In/Out	In	In	In/Out	In/Out	In/Out		In	In/Out		In			In	In / Out	In
<b>RESPONSE SERVICES</b>																	
Cyber Security Incident Management	In	In/Out	In	In	In/Out	In	In/Out	In/Out	In	In/Out		In			In	In/Out	In
Cyber Security Incident Response - Tier 1 (first response)	In	In/Out	In	In/Out	In/Out	In	In/Out	In/Out	Out	In/Out		In			In	In	In
Cyber Security Incident Response - Tier 2 (troubleshoot)	In/Out	In/Out	In	In	In/Out	In	In/Out	In/Out	In	In/Out		In			In	In/Out	In
Cyber Security Incident Response - Tier 3 (large scale)	In/Out	In/Out	In	In	In	In	In/Out	Out	In	In		In/Out			In	Out	Out
Forensic Investigation - Malware Infections	Out	In/Out	In	In/Out	In/Out	In/Out	In/Out	Out	In	In		In/Out			In	Out	In
Forensic Investigation - Information Breach	Out	In/Out	In	In/Out	In/Out	In/Out	In	Out	In	In		In/Out			In	Out	In
Forensic Investigation - Digital threat to staff (work)	Out	Out	In	In/Out	In/Out	In	In	Out	In	In		In/Out			In	Out	In
Forensic Investigation - Digital threat to staff (personal)	Out	Out		In/Out	In/Out			Out									
Forensic Investigation - Suspicious systems/data activity	Out	In/Out	In	In/Out	In/Out	In	In	Out	In	In		In			In	In/Out	In
Forensic Investigation - Staff performance matters	Out			In	In/Out	In	In	Out		In		In			In	In/Out	In
<b>RECOVERY SERVICES</b>																	
IT Disaster Recovery Program Management	In	In	In	In	In	In	In	In/Out	In	In		In				In	In
IT Disaster Recovery Exercise Coordination	In		In	In	In/Out	In	In	In/Out	In			In				In	In
IT Disaster Recovery Program Training	In		In		In/Out	In	In	In/Out	In			In				In	In
IT Disaster Recovery Program Compliance & Reporting	In		In	In	In	In	In	In/Out	In			In				In	In
Business Continuity Planning & Coordination	In	In	In	In	In/Out	In	In	In/Out	In	In		In				In	In/Out
<b>PLANNING AND AWARENESS SERVICES</b>																	
Online Cyber Security Awareness Program	In	In/Out	In/Out	In/Out	In/Out	In	In	In	In	In		In			In/Out	In	In
Inclass Cyber Security Awareness Program					In/Out	In	In	In	In			In					
Cyber Security Professionals Training Program		Out	In		In/Out	Out	In	In	In	In		In			Out	Out	Out
Cyber Security Policies & Standards Development	In	In	In	In	In/Out	In	In	In	In	In		In			In	In	In/Out
Cyber Security Policies & Standards Compliance	In	In	In	In	In/Out	In	In	In	In	In		In			In	In	In
Cyber Security Operations Reporting	In	In	In	In/Out	In/Out	In	In	In	In	In		In			In	In / Out	In
Cyber Security Program Planning	In	In	In	In/Out	In/Out	In	In	In	In	In		In			In	In	In
Development of Security Tools		In / Out			In/Out	In	In	In	In								Out
Cyber Security Consulting & Advisory Services	In/Out	In/Out	In	In/Out	In/Out	In/Out	In	In/Out	In	In		In / Out			In / Out	In / Out	In
Cyber Security Outreach (liaison with other orgs.)	In	In	In	In	In	In	In	Out	In	In		In			In	In	In
Product Evaluation or Certification		Out	In			In/Out	In	Out	In	In		In / Out			In	In	In/Out





# Top 3 Cyber Threats to FPT

## ► Vulnerabilities Resolution:

- CCCS and other threat intel organizations provide daily notification of vulnerabilities along with criticality and resolution assistance. Many organizations also perform their own vulnerability scans. However, most organization struggle to resolve critical vulnerabilities in a timely manner due to lack of resources or high workload, resulting in significant unnecessary risks to our organizations.
- Most vulnerabilities are with legacy systems and unpatched infrastructure.
- Examples: Alberta, 9,000+ critical vulnerabilities; MISA Prairies, 3,000+ critical vulnerabilities.

## ► Attracting and Retaining Qualified and Experienced Cybersecurity Personnel:

- There is a worldwide cybersecurity talent shortage. It has become increasingly difficult to find talent and all organizations are competing to attract the same talent. To compound the issue, Canadian public sector organizations' remunerations are no longer competitive,.
- Examples: British Columbia, 3 premium openings; Alberta, 13 vacant FTEs out of 53 (6 for more than 6 months).

## ► Cybersecurity Operational Technologies (OT):

- Operational technology cybersecurity is the software, hardware, practices, personnel, and services deployed to protect infrastructure, people, and data. OT investment capabilities are different across all organizations, and there are no standard compliance mechanism to help organizations compare themselves to a best practice, providing direction to ensure that they are ready to face the world's evolving cyber threat.



# Additional Identified Cyber Threats to FPT

- ▶ **Lack of cyber threat awareness:**

- ▶ Still to this day, people don't seem to be aware of cyber threats, even when training is in place. There is a general feeling that the organization staff are working for can and will handle all cyber threats.

- ▶ **Growth of our attack surface:**

- ▶ The COVID-19 pandemic had the positive effect of fast-tracking the digitization of most governments' services as well as the adoption of more mobile technologies. The number of outward-facing applications, the increase in number of mobile users, and the growing (sometimes unknown) use of cloud services make it challenging to ensure that proper controls are in place to protect digital assets.



# Top 3 Common FPT Cybersecurity Activities

## ► Incident Response:

- As organizations are facing increasing challenges in identifying, attracting and retaining staff, most have to increase their focus on basic and reactive cybersecurity incident response – impacting their ability to enhance their environment and shift to a more proactive threat management approach.

## ► Vulnerabilities Management:

- Vulnerabilities management is the highest threat to our organizations. Most jurisdictions are currently focused on finding ways to improve their vulnerabilities resolution capabilities.

## ► Standardize and modernize Cybersecurity Operational Technology:

- Most jurisdictions have grown their cloud presence and their ability to work remotely over the past few years. This has greatly impacted their ability to protect their digital assets and detect security events directed at their assets. As a result, all jurisdictions are looking at ways to quickly evolve and adapt their cybersecurity toolset to one that can monitor end-points and services, beyond the traditional peripheral controls that might have been enough to protect their environments a few years ago.





# Additional Common FPT Cybersecurity Activities

- ▶ **Expansion of Cybersecurity Programs to external jurisdiction stakeholders:**
  - ▶ Quebec, Ontario, Manitoba, British Columbia, and Alberta are all looking at expanding their cybersecurity programs to external jurisdiction stakeholders with a goal of strengthening their overall jurisdiction cybersecurity postures, and in most cases, with a focus on developing new cybersecurity talent.
- ▶ **Asset Management and Configuration Management Database:**
  - ▶ Many organizations looking at implementing new tools to bring together disparate asset management practices into a cohesive central repository that may also identify relationships and dependencies amongst assets.
- ▶ **Proactive digital fraud detection:**
  - ▶ Many jurisdictions have now committed to a digital government services by default approach. This increases the potential for digital fraudulent activities. Many jurisdictions are now researching digital user behavior analysis tools to proactively detect and assess suspicious activities.
- ▶ **IMT control framework:**
  - ▶ Many organizations are currently implementing or adapting their standard maturity-based IMT controls framework to measure compliance to standard IMT security controls. These frameworks will be leveraged to identify weaknesses in the environment that must be addressed in a timely manner, as well as to assist to prioritize digital work.
- ▶ **Privileged Access Management:**
  - ▶ Some organization are dealing with issues regarding elevated privilege accounts. Current practices are being assessed with a goal to enable tools and process to secure the use of privileged accounts.





# Proposal: Attraction and Retention of Cybersecurity Personnel (See Attached Proposal)

- ▶ Issue:
  - ▶ Cybersecurity teams across the Canadian public sector are facing serious staffing issues, having difficulties in identifying, attracting, and retaining qualified and experienced cybersecurity professionals.
- ▶ Purpose of the Proposal:
  - ▶ Identify funding and a partner to complete a study to resolve the issue.
  - ▶ The study should include:
    - ▶ A comparative analysis of the criticality of the problem across jurisdictions
    - ▶ An analysis of cybersecurity compensation expectations across public and private organizations in each jurisdiction
    - ▶ A recommendations to improve the ability of our organizations to attract and retain cybersecurity talent for each jurisdiction
  - ▶ Identified partner will work with jurisdictions' cybersecurity leads via the National CISO Subcommittee on Information Protection (NCSIP).



# Discussion: NCSIP Reporting Relationship to PSCIOC

- ▶ Cybersecurity is a core issues for all jurisdictions who are currently adopting a digital by default approach.
  - ▶ Deputy Minister Councils often discuss cybersecurity and privacy at their meetings, and often request their Cybersecurity leads to attend.
  - ▶ New Minister/Deputy Minister table on Cybersecurity created in June 2022.
- ▶ For many years, private sector organizations have had their CISOs at the same level as their CIOs and CTOs
  - ▶ Many jurisdictions have followed suite, such as Alberta, Ontario, Manitoba, Quebec, with more jurisdictions currently considering it.
- ▶ Quebec, Ontario, Manitoba, British Columbia, and Alberta are expanding their cybersecurity programs to external stakeholders, beyond the control and authority of their CIOs.
- ▶ **Question:**
  - ▶ Should the National CIO Subcommittee on Information Protection (which should already be renamed to National **CISO** Subcommittee on Information Protection), become a full-fledged committee (National **CISO** Committee on Information Protection), with a goal to support the new Minister/Deputy Minister table on Cybersecurity?



Classification: Protected A