



# National CISO Committee on Information Protection (NCCIP)

State of FPT Cybersecurity

PSCIOC CONFERENCE – FEBRUARY 2023



# AGENDA

- ▶ BC FPT Symposium on Digital Trust
- ▶ FPT Jurisdictions – Cybersecurity Capabilities Matrix
  - ▶ Cybersecurity Frameworks Used
  - ▶ Supported Stakeholders
  - ▶ Services Capabilities
  - ▶ Artefacts in Place
- ▶ NCCIP 18-Months Action Plan



# BC FPT Symposium on Digital Trust

- ▶ For two full days, we had the attention of most FPT Ministers and Deputy Ministers in charge of digital and cybersecurity services
- ▶ Extremely well supported and coordinated conference
- ▶ Cybersecurity panel discussion resulted in two action requests:
  1. Ministers and Deputy Ministers for Digital/Technology/Cybersecurity should approach their counterparts on the post-secondary education side asking what they are doing to assist with the development of cyber and digital talent.
  2. Ministers and Deputy Ministers table support is requested to establish a more timely cybersecurity information sharing / communication framework for sharing critical information amongst FPT cybersecurity teams.
- ▶ One more item brought up for future consideration: potential for a national cybersecurity response centre



# FPT Cybersecurity Capabilities Matrix Cybersecurity Frameworks

Jurisdictions		Employed Standard	Aligned/ Complied/ Certified	Comments
Provinces	NL	ISO/IEC 27000	Aligned	Originally used ISO/IEC 27001, but migrated to NIST in 2021
	NS	NIST Cybersecurity Framework	Aligned	Originally used ISO/IEC 27001, but migrated to NIST in 2016. Maturity scoring model used to gauge compliance.
	NB	PolicyPro (COBIT based)	Aligned	PolicyPro (based on COBIT), PCI/DSS. There are a few other pockets of adoption including ISO 27000. PCI/DSS compliant.
	PEI			
	QC	ISO/IEC 27000, COBIT, NIST Cybersecurity Framework	Aligned	Not following one specifically, but a few are used to develop policies. Policies are aligned to these standards.
	ON	ISO/IEC 27002, NIST Cybersecurity Framework	Aligned	Not following one specifically, but a few used to develop policies. Standard stack is a complete mapping against ISO/IEC 27002 controls and the cloud adoption security model is a mix of NIST SP 800-53 and ISO 27017/27018. No certification on the standards, but internal audit verified ISO/IEC 27002 compliance a few years ago.
	MB	NIST Cybersecurity Framework	Aligned	Recent refresh of all NIST Policies and Standards
	SK	ISO/IEC 27000	Aligned	No certification. Self assessed policies are aligned.
	AB	NIST Cybersecurity Framework	Aligned	Moving away from ISO/IEC 27000. Internal Information Security Management Directives are aligned to NIST controls and maturity compliance is used to verify progress towards compliance. PCI/DSS compliance is Treasury Board and Finance owned and led.
	BC	NIST Cybersecurity Framework	Aligned	Implemented policies were originally based on ISO/IEC 27000. Annual information security reviews are based on the NIST framework.
	YT	ISO/IEC 27000	Aligned	YGISP based on ISO standards
	NT	ISO 27001/ISF	Aligned	Own set of standards based on ISO and ISF
	NU			
*MISA	Atlantic			
	East	NIST Cybersecurity Framework, Policy Pro, ISF Standards, COBIT 4	Aligned	Developed own policies based on stated standards. Not certified.
	Prairies	NIST Cybersecurity Framework	Aligned	No certification, but policies are aligned and assessments are performed annually by a 3rd party.
	West	NIST Cybersecurity Framework	Aligned	Using framework to develop internal policies.





# FPT Cybersecurity Capabilities Matrix Supported Stakeholders

														*MISA			
	NL	NS	NB	PEI	QC	ON	MB	SK	AB	BC	YT	NT	NU	Atl	East	Prair	West
Jurisdiction Organization Itself	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓
Jurisdiction Cabinet or Council	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓			✓	✓	✓
Police Force	✓	!	!		!	✓	!	!	!	!					✓	!	!
Worker's Compensation Board		!	~	!	!	!	!	~	~	!		!					
Hospitals	!	✓	✓	✓	✓	✓	!	~	~	~		✓					
Medical Clinics	!	!		✓	✓	~	!		~			✓					
K-12 School Boards	~	!	~	✓	✓	~	!	!	~	✓		~					!
K-12 Schools	~	!	~	✓	✓	!			~	✓		~					
Post-Secondary Institutions	!		!		✓	!			~	✓		~				!	
Power Utility Providers/ Power Grids	!		~		!	!		!	~	~		!				✓	
Oil Industry/ Refineries/ Oil Transport	!					!			~	!							
Water & Sewage Utility Providers						!			~	!		!			✓	✓	!
Jurisdiction - Other Public Agencies	~	!	!	!	!	~	~	~	~	!		~				!	!
Municipal Governments within Jurisdiction			!	!			!	~	~	✓		~			✓		
Estimated Supported Stakeholders	8,500	60,000	45,000	8,000	510,000	75,000	18,000	14,000	35,000	32,000	5,000	5,500			5,000	2,000	1,600
LEGEND:																	
- Provide cyber security service (directly)	✓																
- Provide advice and some oversight (arms' length)	~																
- No support, but relationship exists (communication)	!																



# FPT Cybersecurity Capabilities Matrix

## Services Capabilities

### PART 1

															*MISA		
	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	3	18	9	3	32	65	5	16	56	51	5	4			4	2	1.5
Additional Cyber Security Staff across Organization	1	1	17	0	28	30	1	0	0	26	0	0			0	0	0
TOTAL Cyber Security Staff within Jurisdiction	4	19	26	3	60	95	6	16	56	77	5	4	0	0	4	2	1.5
Supported Stakeholders per Cyber Security Staff	2,125	3,158	1,731	2,667	8,500	789	3,000	875	625	416	1,375	1,375			1,250	1,000	1,067
THREAT IDENTIFICATION & ASSESSMENT SERVICES																	
Security Threat & Risk Assessment	In/Out	In/Out	In/Out	In/Out	In/Out	In	In	In	In	In/Out	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	In
Vulnerability Scanning - Infrastructure based	In/Out	In/Out	In	In	In/Out	In	In	In	In	In	In	In/Out			In	Out	In
Vulnerability Scanning - Application based	In/Out	In/Out	In	In/Out	In/Out	In/Out	In	In	In	In/Out	In	In/Out				Out	In
Vulnerability Management and Reporting	In	In	In	In	In/Out	In	In	In	In	In	In	In			In	Out	In
Cyber Threat Intelligence Research	In/Out	In/Out	In/Out	In/Out	In/Out	In	In/Out	In/Out	In	In/Out	Out	In/Out				In/Out	In/Out
Cyber Threat Intelligence Reporting	In	In/Out	In	In	Out	In		In	In	In/Out	Out	In/Out				In/Out	In/Out
PROTECTION & DETECTION SERVICES																	
Security Operations Centre Services	Out	In/Out	In	Out	In/Out	In	In/Out	In/out	In/Out	In	Out	Out			In	Out	
Firewall Management	In	In	In	In	In/Out	In/Out	In/Out	In/out	Out	In	In	In			In	In	In
End Point Management - Servers	In	In	In	In	In/Out	In/Out	Out	In/out	In	Out	In	In			In	In	In
End Point Management - Desktops	In	In	In	In	In/Out	In/Out	Out	In/out	In	Out	In	In			In	In	In
End Point Management - Mobile Devices	In	In	In	In	In/Out	In/Out	Out	In/out	In	Out	In	In			In	In	In
Antivirus Management - Servers	In	In	In	In	In/Out	In	Out	In/out	In	Out	In	In			In	In	In
Antivirus Management - Desktops	In	In	In	In	In/Out	In	Out	In/out	In	Out	In	In			In	In	In
Antivirus Management - Mobile Devices	In	In	In	In	In/Out	In	Out	In/out	In	Out	In	In			In	In	In
Network Traffic Monitoring	In	In	In	In/Out	In/Out	In	In/Out	In/out	In/Out	In	In/Out	In			In	In / Out	In
Host Log Monitoring	In	In/Out	In	In/Out	In/Out	In	In/Out	In/out	In/Out	In/Out	In/Out	In				In/Out	In
Security Information Event Monitoring (SIEM)	Out	In	In	In/Out	In/Out	In	In/Out	In/out	In/Out	In/Out	In/Out	In/Out				In/Out	In
Cloud Services Access Monitoring	Out	In/Out	In	In	In/Out	In/Out		In/out	In/Out		In/Out				In	In/Out	In
Implementation & Configuration of Security Controls	In	In/Out	In	In	In/Out	In/Out	In/Out	In/out	In	In/Out	In	In			In	In / Out	In



# FPT Cybersecurity Capabilities Matrix

## Services Capabilities

### PART 2

														*MISA			
	NL	NS	NB	PEI	QC	ON	MB	SK	AB	BC	YT	NT	NU	Atl	East	Prai	West
RESPONSE SERVICES																	
Cyber Security Incident Management	In	In/Out	In	In	In/Out	In	In/Out	In/Out	In	In/Out	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	In
Cyber Security Incident Response - Tier 2 (troubleshoot)	In/Out	In/Out	In/Out	In	In/Out	In	In/Out	In/Out	In/Out	In/Out	In	In			In	In/Out	In
Cyber Security Incident Response - Tier 3 (large scale)	In/Out	In/Out	In/Out	In	In	In	In/Out	Out	In	In	In/Out	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	Out	In
Forensic Investigation - Information Breach	Out	In/Out	In	In/Out	In/Out	In/Out	In	Out	In	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	Out	In
Forensic Investigation - Digital threat to staff (personal)	Out	Out		In/Out	In/Out			Out	In			In/Out					
Forensic Investigation - Suspicious systems/data activity	Out	In/Out	In	In/Out	In/Out	In	In	Out	In	In	In/Out	In/Out			In	In/Out	In
Forensic Investigation - Staff performance matters	Out			In	In/Out	In	In	Out		In	In				In	In/Out	In
RECOVERY SERVICES																	
IT Disaster Recovery Program Management	In	In	In	In	In	In	In	In/Out	In	In	In	In				In	In
IT Disaster Recovery Exercise Coordination	In		In	In	In/Out	In	In	In/Out	In		In	In				In	In
IT Disaster Recovery Program Training	In		In		In/Out	In	In	In/Out	In		In	In				In	In
IT Disaster Recovery Program Compliance & Reporting	In		In	In	In	In	In	In/Out	In		In	In				In	In
Business Continuity Planning & Coordination	In	In	In	In	In/Out	In	In	In/Out	In	In	In	In				In	In/Out
PLANNING AND AWARENESS SERVICES																	
Online Cyber Security Awareness Program	In/Out	In/Out	In/Out	In/Out	In/Out	In	In	In	In	In	In/Out	In			In/Out	In	In
Inclass Cyber Security Awareness Program					In/Out	In		In	In								
Cyber Security Professionals Training Program		Out	In		In/Out	Out	In	In	In	In		In/Out			Out	Out	Out
Cyber Security Policies & Standards Development	In	In	In	In	In/Out	In	In	In	In	In	In/Out	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	In
Cyber Security Operations Reporting	In	In	In	In/Out	In/Out	In	In/Out	In	In	In	In	In/Out			In	In / Out	In
Cyber Security Program Planning	In	In	In	In/Out	In/Out	In	In/Out	In	In	In	In/Out	In			In	In	In
Development of Security Tools		In/Out			In/Out	In	In/Out	In	In								Out
Cyber Security Consulting & Advisory Services	In/Out	In/Out	In	In/Out	In/Out	In/Out	In/Out	In/Out	In	In	In/Out	In / Out			In / Out	In / Out	In
Cyber Security Outreach (liaison with other orgs.)	In	In	In	In	In	In	In	In	In	In	In	In			In	In	In
Product Evaluation or Certification		Out	In			In/Out	In	In	In	In	In	In / Out			In	In	In/Out



# FPT Cybersecurity Capabilities Matrix Artefacts In Place

															*MISA			
	NL	NS	NB	PEI	QC	ON	MB	SK	AB	BC	YT	NT	NU	Mar	East	Prai	West	
One Over-arching Cyber Security Policy	✓	!	✓	✓	✓	✓	✓	✓	✓	✓	!	✓				✓	!	
Internal Cyber Security Policies or Directives	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	!	✓			✓	✓	!	
Internal Cyber Security Standards	✓	✓	✓	!	✓	✓	✓	✓	✓	✓	!	✓				!	✓	
Policy stating what is an official record (source of truth)		✓	✓		✓	✓		!	✓			✓			✓	!	✓	
Actual stated source of truth ( <u>digital</u> / <u>paper</u> / <u>undefined</u> )		p/d	p/d		!	p/d		u	d	p/d		p/d			p	u	p/d	
Data/Information Security Classification Standard	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓				!		
Cyber Security Strategy	✓	✓	✓	!	!	✓	!	✓	✓	✓	✓	!				✓	!	
Cyber Security Program/Services Plan (3 years+)		✓	✓		!	✓	!	✓	✓	✓	!	!			✓	✓	!	
Security Risk Management Framework/Practice	✓	✓	✓		✓	✓	✓	✓	✓	!	!	!			!	!	!	
Enterprise Security Risk Register		✓	✓	!	✓	✓	!	✓	✓	✓	✓	!			!	!		
IT Disaster Recovery Framework/Practice	✓	✓	!	!	✓	✓	✓	✓	✓	!	!	!			!	✓	!	
IT Applications and Systems Inventory	✓	!	!	✓	✓	✓	✓	✓	✓	✓	!	!			✓	!	✓	
Prioritized List of Application (Criticality Classification)	✓	!	!	✓	!	✓	✓	✓	✓	✓		!			✓	!	✓	
Configuration Management Database	✓	!	!	!	✓	✓		✓	✓	!	!					!	✓	
Annual Enterprise-wide IT Disaster Recovery Test					!	✓		!	✓							!	!	
Cloud Security Strategy	!	✓	!	✓	!	!	!	!	✓	!		!				!	!	
Cyber Security Operations Reports - Monthly/Quarter	✓	✓	✓	!	✓	✓	✓	✓	✓	✓	✓	✓					!	
Cyber Security Operations Reports - Ad hoc	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓			✓	✓	✓	
Cyber Security Intelligence Reports - Monthly/Quarter			✓		!	✓		✓	✓			!						
Cyber Security Intelligence Reports - Ad hoc	✓	!	✓		!	✓	!	✓	✓			!			✓			
On-line Cyber Security Awareness Program	✓	!	✓	✓	✓	!	✓	✓	✓	✓	!	✓			✓	✓	✓	





# NCCIP 18-Months Action Plan

## ► POSITION PAPERS:

- ❖ Nation State Governments Influence Through Digital Technology and Services (March 2023)
- ❖ Guidelines for Right-Sizing an Organization's Cybersecurity Program (October 2023)

## ► NEW IMPLEMENTATIONS:

- ❖ National Cybersecurity Key Performance Indicators (July 2023)
- ❖ Critical Cybersecurity Information Sharing Framework and Mechanism (Proposal by September 2023 and Implementation by January 2024)
- ❖ Successful Methods for Identifying, Attracting, and Retaining Cybersecurity Talent (Jurisdictions Scan by August 2023 and Implementation by February 2024)

## ► PROPOSAL TO PSCIOC:

- ❖ Requirements and Proposed Plan to Centralize Cybersecurity Incident Response Nationally (November 2023)



# 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.



# Questions?