



NCSIP Response to PSCIOC Requests From the July 2017 Meeting

Prepared on behalf of NCSIP with input from Committee Members by

Martin Dinel, NCSIP Chairperson & Alberta CISO

Robert Samuel, NCSIP Vice-Chairperson & Nova Scotia CISO

Gary Perkins, NCSIP Secretary & British Columbia CISO

September 12, 2017

INTRODUCTION

A review of the October meeting agenda was performed following the NCSIP update at the Public Sector Chief Information Officers Council (PSCIOC) meeting in July 2017. A decision was made to reserve 60 minutes for a NCSIP update on the October 5, 2017 meeting agenda. PSCIOC members identified several topics of interest and asked if NCSIP could assist in providing information for discussion at that meeting:

1. *How are Canadian F/P/T jurisdictions preparing for elections from a cyber security perspective?*
 - a. *What is GeoFencing?*
2. *How can NCSIP assist in keeping CIOs across the country better informed regarding cyber security threats?*
 - a. *Should federal security clearance be obtained to gain access to shared cyber security information?*
3. *How can the government assist in encouraging schools to include cyber security as part of their curriculum?*
4. *What are Canadian F/P/T jurisdictions doing to educate cabinet members, and government employees and contractors in matters of cyber security?*

The following document provides summary answers that will be reviewed in more details during the October 5th PSCIOC meeting.

Participating Jurisdictions included the Government of Canada (GC), Newfoundland & Labrador (NL), Nova Scotia (NS), New Brunswick (NB), Prince Edward Island (PE), Ontario (ON), Manitoba (MB), Saskatchewan (SK), Alberta (AB), British Columbia (BC), Yukon (YT), Northwest Territories (NT), MISA East (ME), MISA West (MW) and MISA Prairies (MP).

No responses provided by Quebec and Nunavut (no representation on NCSIP).



REQUEST #1: HOW ARE CANADIAN F/P/T JURISDICTIONS PREPARING FOR ELECTIONS FROM A CYBER SECURITY PERSPECTIVE?

Only four respondents (YT, NT, PE and ME) reported that they have not started to prepare for their next elections, however, it is likely that related work will be performed in the future.

All other jurisdictions (GC, NL, NS, NB, ON, MB, SK, AB, BC, MW and MP) have commenced preparation for their next elections, including the following activities:

- The above jurisdictions have shared the report issued by the federal government titled “Cyber Threats to Canada’s Democratic Process” and/or a related briefing with their executive management to raise awareness about attacks to and risks surrounding Canada’s democratic process.
- All jurisdictions’ cyber security teams have reviewed the federal government document and taken some steps to improve the cyber security environment before and during their next election, including:
 - **Security threat and risk assessments being performed regarding the identified threat to the election process within each jurisdiction.** Identified risks are assessed from a likelihood and impact perspective, prioritized by risk exposures, mitigations are being determined, and the risks will be tracked and managed through internal risk management processes. (All)
 - **Implementation of Geo-Fencing.** Implementing this security control to block unexpected network traffic (mostly network services other than website browsing, or, http on port 80 and https on port 443) coming from countries outside of Canada. (In place or being implemented: AB, BC, NB, NS, MW, ON; being planned: NL, NT, SK, YT, ; not planned: MB, MP, PE, ME)
 - **Increased cyber security operations monitoring.** Increased cyber security operations monitoring protocols will be followed a few weeks before, during, and after the elections ensuring that any suspicious activity is investigated by cyber security personnel and management. (All)
 - **Cyber Security Response Team on Stand-by.** Cyber security personnel on stand-by during the period of increased monitoring with on-call staff ready to respond to any suspicious activity or incident. (All)
 - **Monitoring threat intelligence feeds.** All jurisdictions have reported that they are or will be monitoring threat intelligence feeds before and during the election process.

Some jurisdictional differences:

- Manitoba does not currently leverage GeoFencing. Manitoba has a restrictive firewall policy that only allows inbound traffic based on HTTP/HTTPS communications, no matter the geographical source of the traffic. This is due in part to inherent challenges with implementing GeoFencing based on technology capability – there is a significant possibility of blocking legitimate web traffic when implementing GeoFencing holistically.
- Ontario is meeting with Federal, Provincial and Municipal partners to develop a strategy as well as incident response plans pertaining to Cyber Events during the Election. The Ontario Provincial Police chairs these meetings.
- Prince Edward Island will commence preparation work regarding this topic as soon as a new Chief Electoral Officer is appointed.



- New Brunswick will be going to the polls in 2018. They have tight security controls around the electronic handling of election information, including training and testing of election officials. They are planning to have online training and testing for the 2018 election.
- During the recent British Columbia election, the focus was not on the technology. Next time, technology will play a greater role. Focus will be given to resolving vulnerabilities identified during the risk assessment that has commenced also leveraging the experience of the most recent election. A contributor to the successful cyber security environment during the recent election was that the contact at Elections BC was willing to have a second set of eyes on the situation, and had an open mind. There were also ‘indirect’ impacts that had to be considered with the media. Articles went live tied to incidents or false information regarding election proceedings. While these were dealt with ad hoc, it became clear that preparation work regarding communications must happen ahead of time during future elections. The recommendation from the British Columbia CISO is to start planning as soon as possible, and offer assistance to people in charge of the election proceedings. Regarding GeoFencing, keep in mind that it is a lot easier to scrutinize 4 ports rather than 65,535. Reduce the number of white-listed ports instead of blocking specific ports. Reduce the number of countries having access to your environment, it improves security and performance. It is also important to look at business needs: Anything that isn’t ports 80/443/25/53 and needs to be open to a foreign country should be the exception and very closely scrutinized, additional controls in place etc. When implementing GeoFencing do it at the outermost perimeter of your network, perhaps even at the service provider.
- Nova Scotia has implemented 3 levels of GeoFencing: Nova Scotia only, Canada only, and North America only. There are 5 applications / services in the Nova Scotia GeoFence, 11 in the Canada GeoFence and 8 in the North America GeoFence. Most of the GeoFences were requested by the owners since they know who uses their application and services.
- Ontario’s GeoFencing is applied “ad hoc” based on the identification of malicious traffic in any particular subnet. During election time, they may block particular geographic locations based on intelligence reports.
- New Brunswick doesn’t make extensive use of this technology, due to the ease of spoofing IP’s. However, we do apply rules for remote access which require 2FA and captcha from certain geographies. We also have proposed (no decision has been made) conditional access profiles for Office 365 which take into account location. At this time, we are really only looking at separating Canadian from non-Canadian traffic. We have not progressed to the point of identifying specific target countries as risks.

1.A: WHAT IS GEOFENCING?

GeoFencing is also often referred to as *GeoLocation Filtering*. It means blocking or filtering out network traffic based on its geographic source. For instance, blocking network traffic coming from China or another country.

GeoFencing does not normally block all network traffic, but rather, specific traffic based on the TCP or UDP ports (network services) being used. For example, internet browsing traffic (ports 80 for http, and 443 for https) are allowed for all countries, enabling users from these countries to browse websites, but other ports such as File Transfer Protocol (port 20 for FTP) used to share files, or Secure Shell (port 22 for SSH) used to administer systems remotely might be blocked since these activities should not come from these countries.

IMPORTANT POINT TO MAKE REGARDING GEOFENCING

More sophisticated attackers are now finding ways of avoiding GeoFencing rules by proxy-ing to systems within the geographic location of target environments, or by spoofing IP addresses.



REQUEST #2: HOW CAN NCSIP ASSIST IN KEEPING CIOs ACROSS THE COUNTRY BETTER INFORMED REGARDING CYBER SECURITY THREATS?

The first point of communication relating to Cyber Security with the CIOs of all jurisdictions is and should be the person in charge of Cyber Security for their jurisdiction (referred to as the CISO or Chief Information Security Officer). NCSIP, CCIRC and other means to connect and discuss cyber security issues are accessed and used by the CISOs across the entire country. Information relating to cyber security will come through direct communication between jurisdiction CIOs and CISOs.

It should be noted that not all CISOs have the same capabilities in terms of what they can communicate to their CIOs. For instance, some jurisdictions collect and produce monthly operations report, other quarterly or bi-annually, and other don't have the capability at all. NCSIP is working with all jurisdictions to determine what a basic set of reporting should be, what the reports should contain, how frequently they should be published, and we are also looking at developing a national report or dashboard that could provide a national picture of the cyber security threat and protection. This is a top priority for the sub-committee this coming year.

The following summary provides an overview of cyber security communication needs and capabilities across the various jurisdictions:

Jurisdictions	The CISO is the CIO	Must inform enterprise CIO	Must inform multiple CIOs	Availability of Operations Reports	Availability of Intelligence Reports
Newfoundland	No	Regular and Ad hoc	Regular and Ad hoc	As requested	As requested
Nova Scotia	No	Regular and Ad hoc	Ad hoc	As requested + bi-annual	As requested + bi-annual
New Brunswick	No	Weekly and Ad hoc	Regular and Ad hoc	Quarterly + Ad hoc	Quarterly + Ad hoc
Prince Edward Island	No	Regular and Ad hoc	No	As requested	As requested
Quebec	NA	NA	NA	NA	NA
Ontario	No	Regular and Ad hoc	Regular and Ad hoc	As requested	As requested
Manitoba	No	Regular and Ad hoc	No	Quarterly + Ad hoc	Quarterly + Ad hoc
Saskatchewan	No	Weekly	No	As requested	As requested
Alberta	No	Monthly and Ad hoc	Monthly and Ad hoc	Monthly + Ad hoc	Quarterly + Ad hoc
British Columbia	No	Regular and Ad hoc	Regular and Ad hoc	As requested	As requested
Yukon	No	Ad hoc	No	As requested	As requested
Northwest Territories	No	Regular and Ad hoc	Ad hoc	As requested	As requested
Nunavut	NA	NA	NA	NA	NA
Government of Canada	No	Regular and Ad hoc	Regular and Ad hoc	As requested	As requested
MISA East	No	Ad hoc	NA	Quarterly + Ad hoc	Quarterly + Ad hoc
MISA Prairies	No	Regular and Ad hoc	No	As requested	As requested
MISA West	Yes	CIO = CISO	No	As requested	As requested



2.A: SHOULD FEDERAL SECURITY CLEARANCE BE OBTAINED TO GAIN ACCESS TO SHARED CYBER SECURITY INFORMATION?

All participating jurisdictions agreed that federal security clearance should be obtained by CIOs and executive levels who are accountable for cyber security to ensure that all information in matters of cyber security can be shared with them.

Current Status:

- Executive Members have clearance (8): GC, MB, AB, ON, NT, BC, NL, NB
- Executive Members have requested clearance (1): PE
- Executive Members without clearance, and not requested (5): SK, YT, MW, MP, ME
- No response (2): Quebec and Nunavut

Some jurisdictional differences:

- In Nova Scotia, the government CIO, CISO and Deputy CISO are all cleared, but do not have secure communications means at this time. A vIPer was installed in a provincial regional office in 2016 for clerk-to-clerk communication, but it has never been used; there is also potential to leverage DND CSNI installed in MARLANT HQ and other DND facilities, or to pursue other secure communication solutions.
- New Brunswick notes that the CIO should not necessarily be the “first to know” in regard to cyber threats or risks, nor should they be expected to dive into the “weeds”, but the clearance is necessary.
- British Columbia and Alberta have secure rooms and encrypted telephone solutions for communication, but cannot confirm that full use/ leverage of benefits of these have been achieved.
- At federal government level, employees at all levels receive the level of clearance commensurate with the information required to perform their functions. The GC CIO has the appropriate clearance (as a condition of employment). The granting of federal government clearances to Provincial, Territorial or Municipal CIOs would facilitate information sharing in the cyber security sphere and is seen as a force multiplier which should be pursued.

Request processes for clearance vary based on the jurisdiction. Some provinces also use the RCMP to provide clearance while others go through the Federal government. The best bet is to talk to your CISO to find out the process to obtain federal clearance. Note that in most cases, the process can take up to 8 months to obtain SECRET clearance. TOP SECRET might take up to 12 months.



REQUEST #3: HOW CAN THE GOVERNMENT ASSIST IN ENCOURAGING SCHOOLS TO INCLUDE CYBER SECURITY AS PART OF THEIR CURRICULUM?

After a quick scan, we found that only 2 jurisdictions (MP, NB) are officially and actively involved in such activities; however, many of the jurisdictions (AB, BC, SK, MW, ME) are somewhat involved due to personal / volunteer involvement from their security personnel.

The two jurisdictions currently officially involved are:

- MISA Prairies – In Lethbridge, MISA Prairies works with primary and post-secondary schools to advocate for a number of initiatives. Security is one of the topics. In reality, it is our school system that is providing leadership in this area.
- New Brunswick – As part of its CyberSmart program, CyberNB is focused on developing both near and long-term national workforce development strategies designed to address a global shortage of cybersecurity professionals. Through the K-12 system, CyberNB is working with education partners to identify and change the curriculum to ensure NB has digitally literate graduates. By partnering with academia, government and industry, CyberNB is identifying the key trends as well as competencies that are needed now and into the future. A recent key success was partnering with Canadian-based Blue Spurs on introducing an IOT education kit in NB schools, culminating with Blue Spurs winning the AWS Global City on Cloud Innovation Award. CyberNB has also been promoting NB middle and secondary school students to participate in the national Cyber Titan program with competitions both here in Canada and in the US. In May of 2017, CyberNB hosted CyberSmart 2017, the first summit in Canada specifically designed to promote collaboration between industry, academia, government and youth on a national cybersecurity workforce development strategy.

Additionally, Public Safety Canada's GetCyberSafe program does not work with schools directly; however, the program collaborates with organizations that do, especially when it comes to content aimed at parents and youth. GetCyberSafe also works with TELUS WISE (Wise Internet and Smartphone Education) program (providing content and GetCyberSafe tip sheets), which has a program of speakers available to schools and parent councils to talk about internet safety. GetCyberSafe recently reached out to university student associations and several of them across Canada have included a GetCyberSafe postcard on the importance of safe online financial transactions (shopping, banking) in frosh week kits. This has resulted in a distribution of over 40,000 bilingual postcards.

Some jurisdictional differences:

- Alberta – The Corporate Information Security Office is currently involved in discussions with one college and two universities to create a cyber security diploma program, which could eventually evolve into a degree program. The Managed Security Service provider for the Government of Alberta, CGI, is also involved in these activities. A Coop-type arrangement is the ultimate target, which would provide work experience to students while also providing resources for program sponsors. No focus on K-12 at this time.
- British Columbia – There are already diploma programs with cyber security specialties in British Columbia, but the ultimate target of the CISO would be a degree program.
- Prince Edward Island – Not involved at this time, but they have suggested that schools look into setting up a program to go along with the introduction of wireless and BYOD in our schools.
- MISA East – The CISO participated in a discussion debating the merits of creating a cyber security Master program (a 4-year INFOSEC/Networking degree program already exists).



REQUEST #4: WHAT ARE CANADIAN F/P/T JURISDICTIONS DOING TO EDUCATE CABINET MEMBERS, AND GOVERNMENT EMPLOYEES AND CONTRACTORS IN MATTERS OF CYBER SECURITY?

All participating jurisdictions have some form of generic cyber security awareness and training program, including access to online resources and in-class presentations. The program is offered to all government employees. Most jurisdictions have a policy that all employees must complete this type of training annually.

List of topics normally covered by the training programs include:

- Email phishing and Social Engineering
- Payment Card Industry standards
- General safe practices while using computer devices
- Safe practices while using mobile devices and WiFi networks
- Information Security Classification / Information Management
- FOIP
- Systems administration security standard practices
- Systems development security standard practices

These awareness programs also often include newsletters or regular participation in corporate newsletters, as well as a focus on Cyber Security Awareness month (every October) using posters and pertinent related activities.

While all jurisdictions agree that an education program for cabinet members is an absolute must, only two jurisdictions (GC and BC) currently have access to their cabinet members. Cabinet members have access to the generic tools made available to other government employees, but reporting in various jurisdictions confirm that they normally don't access this material and rarely are debriefed on the cyber threat.

The CISO for BC has connected directly with caucus to provide general awareness material.

At the Government of Canada, Cabinet members are informed on matters of cyber security through a variety of means, including DM breakfasts, DM Cyber Meetings, and at different executive decision-making bodies as required.

Apart from the above, many jurisdictions "might" get access to cabinet members before they travel to conduct a debrief, but it is not the norm, nor does it happen all the time for these jurisdictions.

It should be noted that this year for the first time, Ontario will get access to senior management and conduct a Cyber War Game exercise with participants from the various ministries.

It is a fact that cabinet members are all excellent targets for malicious threat actors. They are in the public eye and much personal information is often revealed about these people on social media as well as news media. It is critical that cabinet member be informed and made aware of cyber threats that may impact them, and taught how to respond to them.

National CIO
Subcommittee on
Information Protection



IN CLOSING

Should you have any further concerns or questions, please contact one of the NCSIP Officers:

- **NCSIP Chair:** Martin Dinel, Alberta CISO | Martin.Dinel@gov.ab.ca | Phone: (780)427-2429
- **NCSIP Vice-Chair:** Robert Samuel, Nova Scotia CISO | Robert.Samuel@novascotia.ca | Phone: (902)222-6685
- **NCSIP Secretary:** Gary Perkins, British Columbia CISO | Gary.Perkins@gov.bc.ca | Phone: (250)387-7590