UNCLASSIFIED

Government of Canada / Gouvernement du Canada

Canada

Deputy Ministers' Cyber Security Committee
June 24, 2021 – 1:00 pm to 2:30 pm
PCO/CISCO Secure Line
(1.5 hours)

DRAFT AGENDA

Time	Item	Associated Documentation
1. 1:00-1:10 *(10 min)*	**Opening Remarks** Rob Stewart, Deputy Minister, Public Safety Canada Shelly Bruce, Chief, Communications Security Establishment	
2. 1:10-1:35 (*25 min*)	**Ops Brief: Colonial Pipeline and JBS** Objective: Provide background on recent incidents and findings from the June 8 DGCS walk through of an incident in Canada modelled on the Colonial Pipeline incident. Communications Security Establishment Public Safety Canada *For Update and Discussion*	*Document*
3. 1:35-2:00 (*25 min*)	**Canada-US** Objective: Provide an update on the CAN/US efforts on cyber security and discussion regarding the addition of Ransomware as a priority topic on the cyber roadmap Communications Security Establishment *For Update, Discussion and Endorsement*	*Document*
4. 2:00-2:25 (25 *min*)	**Cyber Security Certification in Canada** Objective: DND has identified the need for a Canadian approach to cyber security certification.. We will explore the need for a cross-sector approach to certification. Department of National Defense Public Safety Canada *For Discussion and Endorsement of Next Steps*	*Presentation*
5. 2:25-2:30 *(5 min)*	**Roundtable and Closing Remarks** All	

NON CLASSIFIÉ

Gouvernement du Canada | Government of Canada

Canada

Comité des sous-ministres sur la cybersécurité
Jeudi 24 Juin, 2021 - 13h00 à 14h30
Ligne sécurisé du BCP/CISCO
(1,5 heures)

AGENDA

Durée	Item	Documentation
1. 1:00-1:10 *(10 min)*	**Remarques d'ouverture** Robert Stewart, Sous-ministre, Sécurité publique canada Shelly Bruce, Chef, Centre de la sécurité des télécommunications	
2. 1:10-1:35 (*25 min*)	**Mise à jour sur les cyber-opérations : « Colonial Pipeline » et « JBS »** Objectif : Présenter les faits saillants de récents incidents ainsi que les conclusions de la simulation du 8 juin du CSDGs en prévision d'incidents semblables au Canada. Centre de la sécurité des télécommunications Sécurité publique Canada *Pour mise à jour et discussion*	*Document*
3. 1:35-2:00 (*25 min*)	**CAN/ÉU** Objectif : Fournir une mise à jour sur les efforts CAN/EU en matière de cybersécurité et discuter de l'ajout de rançongiciels comme sujet prioritaire sur la feuille de route cybernétique. Centre de la sécurité des télécommunications *Pour information, décision et entérinement*	*Document*
4. 2:00-2:25 (*25 min*)	**Certification en cybersécurité au Canada** Objectif : Le MDN a identifié le besoin d'une approche pancanadienne pour la certification en cybersécurité. Nous allons explorer les options d'une certification pan-sectoriels. Ministère de la Défence Nationale Sécurité publique Canada *Pour Discussion et entérinement des prochaines étapes*	*Présentation*
5. 2:25-2:30 *(5 min)*	**Table ronde et mot de la fin** Tous	

Public Safety Canada | Sécurité publique Canada

UNCLASSIFIED

Deputy Ministers' Committee on Cyber Security
Thursday, June 24th, 2021 – 1:00 pm to 2:30 pm
PCO Classified Mobile/Cisco System (Secret - Level II)

ANNOTATED AGENDA

1. *Opening Remarks and Agenda for DMCS Meeting*
1:00-1:10 pm (10 min)

Objective: Open the DMCS Meeting.
Speakers: Co-chairs Rob Stewart and Shelly Bruce
Material: Table of Contents, Agenda, List of Participants, Record of Discussion (April 20 meeting)

- Roll-call by department, see list of participants.
- You will have received the Record of Discussion from the last meeting that took place on April 20, 2021. Please provide any comments by COB Monday (28 June), after which it will be considered approved by the Committee.

Today's Agenda:
- Ops Brief: Colonial Pipeline and JBS
- CAN/US
- Cyber Security Certification in Canada

We have included in the meeting package for information:

Forward Policy Plan Dashboard

Speaking Points:

- The dashboard provides an overview of progress of the Forward Policy Plan policy initiatives, approved by DMs last summer.
- We invite you to continue providing us with updates to keep the community apprised of progress, risks and issues.
- We will look more closely at the progress against our Forward Policy Plan when we review results and recommendations for the National Cyber Security Strategy Mid Term Review this fall.

Mid-Term Review Update

Speaking Points:

- We added to the meeting package a 1-pager on the Mid Term Review. This document should give you a glimpse into what our teams are working on and the timelines they are working with to produce a report to signatory ministers by Spring 2022.

- Invite Shelly Bruce, Co-chair to provide introductory remarks.

- Once Shelly's opening remarks are completed, move to item 2

Public Safety Canada | Sécurité publique Canada

UNCLASSIFIED

Move to second item on the agenda: Ops Brief: Colonial Pipeline and JBS

2. *Ops Brief: Colonial Pipeline and JBS*
1:10-1:35 pm (25 min)

Objective: Provide background on recent incidents and findings from the June 8 DGCS walk through of an incident in Canada modelled on the Colonial Pipeline event.
Speakers: Scott Jones
Materials: Documents

- Turn to Shelly Bruce to introduce the item
- Turn to Scott Jones to provide an update on other cyber incidents and results of the walkthrough
- *Open the floor for comments*

Move to the next item on the agenda: CAN/US

3. *CAN/US*
1:35-2:00 pm (25 min)

Objective: Provide an update on the CAN/US efforts on cyber security and discussion regarding the addition of Ransomware as a priority topic on the cyber roadmap.
Speaker: Shelly Bruce
Material: Documents

- Turn to Shelly Bruce

Speaking points: CANADA/US Engagement on Ransomware

- Recent incidents affecting Colonial Pipeline, JBS Meatpacking and Humber River Hospital have demonstrated that ransomware has the potential to pose a threat to public safety and national security.
- The Biden Administration in the United States (U.S.) has made combatting ransomware a priority and a recent Ransomware Task Force Report, released on April 29, 2021, has highlighted the urgent need to take steps to address this issue.
- The Government of Canada (GC) is aware of this issue and has had a Ransomware Working Group (RWG) in place since early 2020. The RWG completed a comprehensive Diagnostique, which was presented to the DM Cyber Committee in the Fall of 2020. The Diagnostique identified a number of gaps in the GC's ability to prevent and respond to ransomware incidents.
- Work to address these gaps remains ongoing. However, given that the threat of ransomware has recently taken on new urgency, a DG Joint Executive Team was formed to provide

coordination and direction to the RWG and develop a coordinated plan to work with the U.S. on this issue.

- The next steps for the RWG are to accelerate ongoing work as identified in the Ransomware Diagnostique and work with [redacted] to develop an action plan for Canada-U.S. collaboration on ransomware.

- We have identified seven areas that we would intend to pursue domestically, and at this time, I am seeking your endorsement to also pursue these as areas of collaboration with the U.S. These proposed areas are outlined in the slides provided to you in your binders:
  - Cyber Insurance
  - Outreach and Engagement Approaches (to improve cyber resilience)
  - Crypto Currency
  - Anti-Money Laundering and Terrorist Financing
  - Incident Response (including walkthroughs or table top exercises;
  - identifying legislative gaps on incident response mandates)
  - Cyber Operations and Law Enforcement Actions (to disrupt cyber
  - criminals)
  - International Engagement

Responsive Only (If asked about Ransomware Task Force Report released in April 2021)

- The RTF Report is one of the most comprehensive studies on ransomware to date. The RWG reviewed its findings to assess the extent to which it should inform the ongoing work of the Ransomware Working Group.

- Review of the RTF report indicated that most of the recommended actions from the RTF report are already being explored as part of the working group or not relevant to the Canadian context. Accordingly, this review confirmed that a large panel of experts in the field of ransomware have not identified anything materially different than what the RWG is already pursuing.

- Issues which exacerbate the spread of ransomware, such as the cyber hygiene of interconnected cyber systems and their users, are not unknown to us; and many such recommendations from the RTF can be matched to existing Government of Canada programs and initiatives.

- In addition, some of the work of the RWG is at more advanced stages of development, such as our engagement strategy for consulting with the cyber insurance industry on issues related to non-disclosure agreements and cooperation with investigation and recovery efforts during ransomware incidents.

- That said, the RTF Report also suggests avenues for further exploration to which the RWG has not yet reached, including policy solutions related to cryptocurrencies and the barriers to information sharing inherent to anonymized currency.

Public Safety Canada | Sécurité publique Canada

UNCLASSIFIED

- The RTF also places appropriate emphasis on the need for international collaboration. Owing to its focus on domestic issues related to ransomware, the RWG has, to date, done limited work related to the international sphere. However, we are looking to ramp up work in this space and leverage our partnership with the Biden Administration to coordinate efforts in this space.

- *Open the floor for comments*

Move to the next item on the agenda: Cyber Security Certification in Canada

4. Cyber Security Certification in Canada
2:00-2:25pm (25 Min)

Objective: DND has identified the need for a Canadian approach to cyber security certification. We will explore the need for a cross-sector approach to certification.
Speakers: Len Bastien,
Materials: Presentation

- Turn to Len Bastien to introduce the item. He will then turn to (DND) and (DND) for the presentation

- *Open the floor for discussion and endorsement of next steps*

5. Closing Remarks
2:25-2:30 pm (5 min)

Objective: Close the DMCS Meeting
Speakers: Co-chairs Rob Stewart and Shelly Bruce

Speaking Points:

- With regard to this meeting's Record of Discussion, a draft will be circulated in the next two weeks and we would appreciate your assistance in replying with your proposed changes, if any, or approval and commitment to deliver on the outlined action items.

- *Summarize action items from this meeting and expected time for delivery.*

- Shelly, do you have final thoughts you'd like to share?
- Would any of you wish to add something or discuss a subject we might have missed?
- The next DMCS is not yet scheduled. Stay tuned for placeholder invitations in the coming weeks.
- I thank you for your attendance and participation.

Public Safety Canada / Sécurité publique Canada

UNCLASSIFIED/ NON CLASSIFIÉ

Deputy Ministers' Committee on Cyber Security
Comité des sous-ministres sur la cybersécurité

Tuesday, April 20th, 2021 – 1:00 pm – 2:30 pm
Mardi, 20 avril, 2021 – 13h à 14h30
Classified Teleconference / Téléconférence classifiée

RECORD OF DISCUSSION / COMPTE RENDU DE LA DISCUSSION
List of Participants / Liste des participants

Member Departments Membres organisationnels	Attendees Participants
Communications Security Establishment Canada – Centre de la sécurité des télécommunications	Shelly Bruce (Co-chair/Co-présidente) Scott Jones
Canadian Security Intelligence Service – Service canadien du renseignement de sécurité	David Vigneault
Department of National Defence – Ministère de la défense nationale	Len Bastien
Finance Canada	Ava Yaskiel
Global Affairs Canada – Affaires mondiale Canada	N/A
Heath Canada - Santé Canada	Harpreet Kochhar
Innovation, Science and Economic Development Canada – Innovation, Science et Développement économique Canada	Simon Kennedy
Justice Canada	Francois Daigle
Natural Resources Canada – Ressource naturelle Canada	Jean-Francois Tremblay
Privy Council Office – Bureau du conseil privé	Vincent Rigby
Pubic Safety Canada – Sécurité publique Canada	Rob Stewart (Co-chair/Co-président) Dominic Rochon
Royal Canadian Mounted Police – Gendarmerie Royale du Canada	Sean McGillis Paul Boudreau [redacted] (presenter)
Treasury Board Secretariat – Secrétariat du Conseil du Trésor	Marc Brouillard
Transport Canada	Aaron McCorie

Public Safety Canada | Sécurité publique Canada

UNCLASSIFIED/ NON CLASSIFIÉ

Record of Discussion

Discussion	Action Items
ITEM 1 – Opening Remarks	
• The Co-chairs provided introductory remarks to members.	
ITEM 2 – EMOTET Takedown	
• RCMP provided a debrief on EMOTET • CSE provided an update on other cyber incidents	Nil
ITEM 3 – CAN/US	
• PCO and NRCan provided an update on recent engagements • DND provided an update on continental defence	Nil
ITEM 4 – Ransomware: Cyber Insurance	
• PS discussed the cyber liability insurance paper. WG is addressing gaps and is leading a deep dive into the issues. • Next steps were discussed, including external consultations. o Timing Fall 2021	PS to begin working through the proposed next steps highlighted in the paper.
ITEM 5- Next Steps: s. 39 - Cabinet Confidence	
• s. 39 - Cabinet Confidence	
ITEM 6 – Roundtable and Closing Remarks	
• The Co-chairs provided closing remarks and noted the next scheduled meeting.	Secretariat to distribute RoDs.

Public Safety Canada | Sécurité publique Canada

UNCLASSIFIED/ NON CLASSIFIÉ

Summary List of Action Items

Agenda Item	Action Item	Lead Department	Expected Date
4	• PS to begin working through the proposed next steps highlighted in the paper.	PS	
5	• PS to share proposed timeline secretarially.	PS	
6	• Secretariat to distribute RoDs	PS	

French follows on next page…

Public Safety Canada / Sécurité publique Canada

UNCLASSIFIED/ NON CLASSIFIÉ

Compte rendu des discussions

Discussion	Points d'action
POINT 1 – Remarques d'ouverture	
• Les coprésidents ont fait des remarques d'ouverture aux membres.	
POINT 2 – Mises à jour opérationnelles, y compris le démantèlement d'« EMOTET »	
• La GRC a fait le point sur EMOTET. • Le CST a fait le point sur d'autres cyberincidents.	NIL
POINT 3 – CAN/É-U	
• Le BCP et RNCan ont fait le point sur leurs récents engagements. • Le MDN a fait le point sur la défense continentale.	NIL
POINT 4 – Ransongiciel : Assurance cyber	
• SP a discuté du document sur l'assurance responsabilité civile cybernétique. Le groupe de travail s'occupe des lacunes et mène une étude approfondie des problèmes. • Les prochaines étapes ont été discutées, y compris les consultations externes. ○ Automne 2021	SP débutera le travail sur les prochaines étapes proposées dans le document.
POINT 5 – s. 39 - Cabinet Confidence	
• s. 39 - Cabinet Confidence	
POINT 6 – Tour de table et mot de la fin	
• Les coprésidents ont donné leurs remarques finales et ont noté la date de la prochaine réunion.	Le Secrétariat distribuera le compte rendu de discussion aux membres

Public Safety Canada | Sécurité publique Canada

UNCLASSIFIED/ NON CLASSIFIÉ

Liste sommaire des mesures à prendre

Point	Point d'action	Ministère responsable	Date prévue
4	• SP commencera le travail sur les prochaines étapes proposées dans le document.	PS	
5	• SP partagera par secrétariat l'échéancier proposé.	PS	
6	• Le Secrétariat distribuera le compte rendu de discussion aux membres.	SP	

CANADIAN CENTRE FOR CYBER SECURITY

Scenario: Cyber Incident Affecting Canadian CI

Key Takeaways

June 2021

Communications Security Establishment | Centre de la sécurité des télécommunications

CERRID XXXXXXXX

Canada

Background

- Ransomware is imposing significant economic costs on companies and disrupting supply chains and the ability of critical infrastructure owners and operators to provide critical goods and services to our citizens.
- CSE's National Cyber Threat Assessment assessed that ransomware "*will almost certainly continue to target large enterprises and critical infrastructure providers*" in Canada.
- The ransomware incident with Colonial Pipeline and the more recent incident involving meat processor JBS SA are having tangible, real-world effects on citizens' lives.
- While the Colonial Pipeline incident did not impact Canada directly, the two countries' integrated energy infrastructure alarmed domestic business and government entities amid fears that future incidents could hit the wider continent.
- To better understand the Canadian response to such an event, the GC undertook a scenario-based walkthrough.

Walkthrough Exercise

- On June 8th, CSE and Public Safety brought together key partners from RCMP, CCCS, DND/CAF, CSIS, NRCan, ISED, GAC, PCO & TBS to conduct a simulated walkthrough inspired by the Colonial Pipeline incident in the United States.

- **Objective:** to identify existing process, authority and legislative gaps as well as any other issues requiring attention, and to increase GC coordination on the diplomatic, policy and operational front to be able to better react/ respond in a rapid manner.

- Response was examined in consideration of a number of factors:
  - Escalation
  - Governance and Decisions
  - Authorities
  - Policies
  - Response leads
  - Information Exchanges
  - Clarity of Roles and Responsibilities
  - Existing Incident Response Processes
  - Communication

Positive Outcomes

- The GC response can build on existing frameworks, coordinating entities, and governance bodies, as well as established networks for communications domestically and internationally
- Some governance exists to help deconflict response actions among federal operational entities, but will require further development. There is no apparent overlap in activities or organizational mandates
- Lead Security Agencies have the authorities to respond operationally (during or post-incident)
- Stakeholders are aware of potential real world pressures (e.g. pipeline disruption leading to gas shortages, political pressure), and therefore better positioned to respond realistically
- GC is already undertaking steps to better prepare for future ransomware occurrences and deter cyber criminals

Notable Gaps

Theme	Gap
Governance, decision making & escalation	• No defined framework for categorization, escalation and coordination of a federal response to a non-federal, CI sector cyber incidents • No clear delineation between cyber emergency and/or broader (all-hazard) emergency • No clear protocol regarding an action-oriented response beyond public attribution • Unclear which interdepartmental governance entities to be invoked
Authorities & policies	• No lever to compel a company or CI operator to report the incident, cooperate with federal & law enforcement agencies, and/or take action • No legislation or policy that prevents the payment of ransom • Challenge with NDAs that do not cover multiple or potential departments or agencies engaged in response at a later point in time • Limited understanding the cyber insurance industry as an enabler • Differing views on whether the distinction between administrative networks vs. operational networks (ICS) changes the federal response to non-federal or CI sector cyber incidents

Notable Gaps

Theme	Gap
Roles and responsibilities & incident response process	• No clear organizational model for coordination of incidents requiring parallel streams of activity (e.g. physical, market impact, cyber security, criminal, national security) • Unclear GC coordination regarding victim notification • Need for pre-existing contingency plans, playbooks and pre-coordination activities • Need to formalize role of GC executives to impress upon implicated companies the importance of cooperation with federal & law enforcement agencies in their response to incidents • No protocol to safeguard the integrity of a cyber incident turned criminal investigation
Information sharing & communication	• Need to expand initial stakeholders to enable activities of secondary departments & agencies • No clarity on which stakeholders receive what information & for what purposes • Need to address limited authority to share critical threat and incident information across law enforcement and security agencies • Need for sector-specific MOUs for information sharing & what caveats exist • Need to coordinate and manage executives' demand for instantaneous information & updates • Need for one lead GC point of communication with the victim • Need for coordinated, structured path and consistent messaging with U.S. & FVEY

Next Steps – Short-Term (Next 6 months)

Domestic:

- Endorsement of one or two additional walkthroughs with Canadian partners on different critical infrastructure scenarios by end of fall 2021
- Establishment of a federal coordination framework to respond to non-federal and CI sector cyber incidents
- Planning for cyber operations and other activities to disrupt cybercriminals and their infrastructure, and to engage CI sectors to defend themselves more effectively
- Building on the work of the Ransomware Working Group, continue analysis and option development on gaps related to:
  - Cyber insurance industry
  - Digital currencies as related to cybercrime
  - Improving incident reporting
  - Public communications and stakeholder engagement

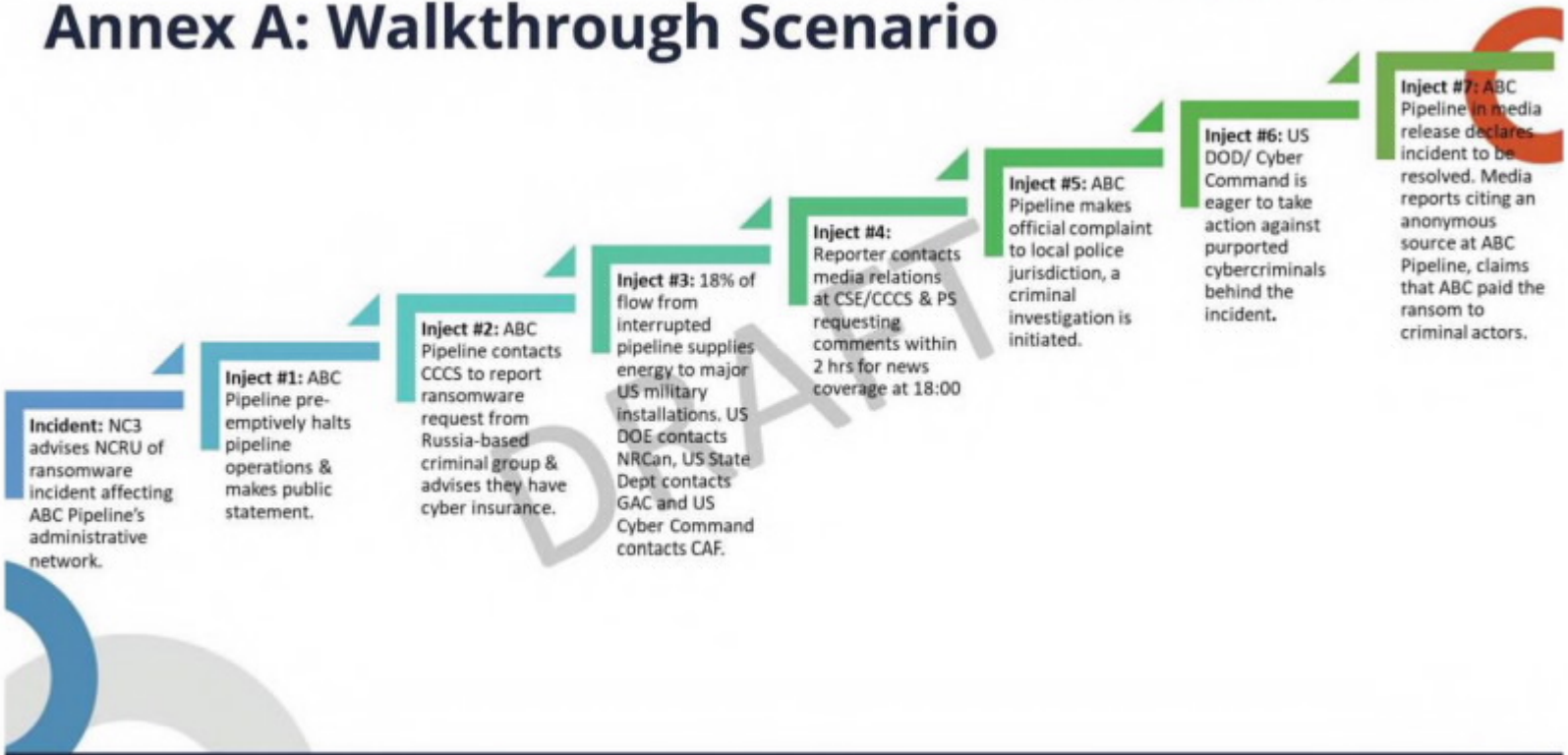
International:

- Work with the US and Five Eyes partners to address ransomware through the
- Proposal for a joint walkthrough with U.S. counterparts on cross-border critical infrastructure scenario

Next Steps – Medium and Longer-Term

- Enhancement of international coordination to:
  - Include partners beyond the Five Eyes to address ransomware, through bilateral and multilateral fora
  -
  - expand capacity and coordination for requests for assistance when incidents occur
- Updating CI regulations (e.g., to compel action, mandatory incident reporting) – starting with Critical Cyber Systems initiative
- Improving Canada's domestic cyber defenses to ransomware attacks across CI sectors, including investigating improved partnerships with the private sector to reduce these threats

Annex A: Walkthrough Scenario



PROTECTED B / PROTÉGÉ B

Current as of 17 June

Deputy Ministers' Cyber Security Committee
CAN-US Activity Brief

1. US Context Development:

(14 June)

Brussels Summit Communique – Cyber-related statements and commitments

- 32. "Cyber threats to the security of the Alliance are complex, destructive, coercive, and becoming ever more frequent. This has been recently illustrated by ransomware incidents and other malicious cyber activity targeting our critical infrastructure and democratic institutions […]"
- 32. "We have today endorsed NATO's Comprehensive Cyber Defence Policy, which will support NATO's three core tasks and overall deterrence and defence posture, and further enhance our resilience."

(13 June)

Carbis Bay G7 Summit Communique – Cyber-related statements and commitments

- 32. Strengthen coordination on and support for the implementation and development of global norms and standards to ensure use and evolution of technology reflects democratic values, open markets, and safeguards human rights and freedoms
- 33. Call on the private sector to join in efforts toward standard setting
- 34. Specific area of cooperation between Digital and Technology Ministers includes "taking further steps to improve internet safety and counter hate speech […]"
- 34. Interior Ministers to work on a "G7 agreement on sharing of information and best practice on tackling existing and emerging online forms of gender-based violence, including forms of online abuse."
- 34. Interior Ministers to continue work on "preventing and countering Violent Extremist and Terrorist Use of the Internet […]"
- 34. "Commit to work together to urgently address the escalating shared threat from criminal ransomware networks [and] call on states to urgently identify and disrupt ransomware criminal networks from operating from within their borders, and hold those networks accountable for their actions."
- 34. "[…] promote secure, resilient, competitive, transparent and sustainable and diverse digital, telecoms, and ICT infrastructure supply chains."
- 48. Commit to "increase cooperation on supporting democracy […] to counter foreign threats to democracy including disinformation […]"

(10 June)

- Confirmation hearings for Chris Inglis (National Cyber Director) and Jen Easterly (CISA Director)

(9 June)

- Executive Order on Protecting Americans' Sensitive Data from Foreign Adversaries issued
  - Secretary of Commerce tasked with developing two reports:

- 1) Within 120 days, recommendations to protect against harm from the unrestricted sale, transfer or access to persons' sensitive data;
  - Within 60 days, related threat and vulnerability assessments will be provided by the Director of National Intelligence and Secretary of Homeland Security to support development of the report and recommendations
- 2) Within 180 days, recommendations of additional executive and legislative actions to address risks associated with connected software applications associated with foreign adversaries
- US Administration has signaled interest in developing coordinated approaches

(8 June)

- Software supplier used by dozens of House offices on Capitol Hill is latest reported high-profile ransomware incident

(8 June)

- US Administration announces key findings from comprehensive 100-day supply chain assessments of four critical products (semi-conductors, batteries, critical minerals, pharmaceuticals) as initiated in 24 February EO entitled "America's Supply Chains".
  - Confirmed next steps (of interest to Canada) include:
    - Secure an end-to-end domestic supply chain for advanced batteries
    - Launch of *Supply Chain Disruptions Task Force* as part of whole-of-government effort to monitor and address transitory supply chain challenges
  - Recommendations to US Administration (of interest to Canada) include:
    - Establish a new *Supply Chain Resilience Program* at DOC to monitor and address supply chain challenges
    - Leverage the government's role as a purchaser and investor in critical goods
    - Develop a comprehensive trade strategy to support fair and resilient supply chains
    - Work with allies and partners to decrease vulnerabilities in global supply chains

(7 June)

- US DOJ announces reclaiming of majority of ransom paid to DarkSide; credits Colonial for quickly notifying and cooperating with FBI following ransomware incident

(3 June)

- US DOJ issues memo to all federal prosecutors with new requirements relating to ransomware investigations, effective immediately, that include the following actions:
  - Notification to Computer Crime and Intellectual Property Section (CCIPS) upon opening a new investigation
  - Filing an Urgent Report upon opening a new investigation

(3 June)

- Executive Order on Investments into certain Companies of the People's Republic of China issued extending a Trump administration EO.
  - The EO prohibits the purchase or sale of any publicly traded securities or derivatives of securities designed to provide investment exposure to a list of PRC entities identified to be involved in military, intelligence, security, surveillance and/or weapons R&D or production.
  - The list of entities under the revised executive order amounts to nearly 60 companies.

Current as of 17 June

(1 June)

- A "Public Wireless Supply Chain Innovation Fund" and "Multilateral Telecommunications Security Fund" have been established through the *National Defence Authorization Act of 2021* to support development and adoption of secure telecom technologies.

(28 May)

- Security Directive on Pipeline Cybersecurity issued by DHS pertains to owners/operators of pipelines deemed critical infrastructure by the Transportation Security Admin. (TSA)
  - Directive requires owner/operators to report cyber incidents to CISA, designate an on-call coordinator for incident response, and review current practices against TSA's cybersecurity recommendations.
  - A second and related Directive expected in June/July 2021

(12 May)

- Executive Order on Cybersecurity issued focusing heavily on cyber resilience and critical infrastructure protection in public and private spheres
- The EO details immediate actions to be taken in the areas of:
  a) sharing of threat information between private entities and federal depts and agencies;
  b) adoption of modern cyber security best practices across federal depts and agencies;
  c) supply chain security in critical software;
  d) creation of a Cyber Safety Review Board to review incidents with a view to vulnerabilities, mitigations and response;
  e) improving detection of cyber vulnerabilities on federal networks;
  f) improving federal investigation and remediation capabilities, and;
  g) bolstering National Security Systems security requirements.

(April)

- The Pentagon pushed back rollout of its Cybersecurity Maturity Model Certification (CMMC) program as it seeks to obtain additional third-party assessment organizations.
  - The CMMC is the new cyber security certification all defence contractors will require in order to bid on contracts.

(March)

- The Biden administration has publicly indicated its intention to attribute the large-scale Microsoft Exchange Server exploitation in the "near future" as it continues to urge organizations to install critical security patches.
  - Microsoft itself attributed the 0-day exploits campaign with "high confidence" to HAFNIUM, a group it assessed to be state-sponsored and operating out of China, on 2 March 2021.
  - This campaign comes on the heels of another significant compromise. On 15 April 2021, the US publicly attributed the SolarWinds Orion Platform supply chain compromise to Russian state-sponsored actors and announced a series of measures to respond to Russian malicious actions, including sanctions and the expulsion of Russian diplomats.
  - This attribution was supported by Canada and a broad coalition of international likeminded countries, and the US is likely to pursue a similar approach in the Microsoft Exchange case.

Current as of 17 June

2. CAN Context Development:

(14 June)

- PM Trudeau met with NATO Secretary General Jens Stoltenberg; PM Trudeau communicated:
  - 1) The importance of allied unity against Russian aggression and challenges posed by China;
  - 2) Canada's continued support to NATO's work on climate change and security, including Canada's interest in hosting a NATO Centre of Excellence (COE) on Climate and Security, and;
  - 3) Canada's continued commitment to the provision of cyber effects to NATO.
- NATO Allies endorsed the new NATO Comprehensive Cyber Defence Policy, among other Action Plans and tasks

(11 June)

- PS hosting bi-weekly DG-level meetings on ransomware to support the coordination of Canada's response to ransomware. Their first meeting included representation from PS, RCMP, NC3, CSE, CSIS, GAC and NRCan; future calls are anticipated to include more departments and agencies.

(9 June)

- PS continues to lead the interdepartmental Ransomware Working Group to develop policy and operational solutions to the threat of ransomware based gaps identified by their *Ransomware in Canada Diagnostique*. The group's most recent meeting was used to deliver updates on the progress of the working group, debrief on new developments, and formulate next steps for developing actionable policy options in the short term.

(4 June)

- PS, RCMP and CSE are leading the development of three ransomware policy documents pertaining to defence of GC networks and areas for multilateral, national and departmental action. The documents will aim to provide policy recommendations in regards to: federal leadership and coordination surrounding ransomware incidents; the jurisdictional and prosecution challenges of pursuing ransomware actors; and the cyber resilience of Canadians and Canadian businesses

(June)

- GAC leading joint demarche to third-party countries (e.g. South America) on the threat of ransomware and state-harbouring of cyber criminals
- Regulatory system for baseline cybersecurity across four critical infrastructure sectors (telecommunications, finance, energy and transportation) and enhanced supply chain security mechanisms for telecommunications infrastructure proposed through Securing Canada's Telecommunications System (SCTS) and Critical Cyber Systems (CCS) MCs—decision with Prime Minister

(May)

- s. 39 - Cabinet Confidence
- Supply chain analysis priorities moving forward, including pursuit of joint CANUS-analysis, as per DG Working Group on Jobs and Economy

Current as of 17 June

(April)

- PS pursuing PS-DHS development of Strategic Framework and Action Plan for Critical Infrastructure
- PS actively engaging US counterparts on joint threat assessment on the Energy Sector

3. Review of items agreed between PM-POTUS

CYBERSECURITY PRIORITIES: CANADA-US ROADMAP		
A.	(Bolstering Security and Defence, 39) **Deliverable:** Increase cooperation to strengthen cybersecurity, and to confront foreign interference and misinformation.	Minister of Public Safety **Joint activities:** • PS-led interdepartmental Ransomware Working Group is focused on developing policy options that could contribute to joint-CANUS activity, drawing on US actions including the Institute for Security and Technology Ransomware Task Force report. • • • GAC collaboration continues within the Freedom Online Coalition (FOC) to shape global norms on Internet Freedom and push back against digital authoritarianism; Canada is the incoming 2022 FOC chair and will work closely with the US and Finland as co-leads
B.	(Bolstering Security and Defence, 36) **Deliverable:** Enhance cooperation to counter exploitation of social media and the Internet by terrorists, violent extremists, and hate groups, strengthen information sharing, and enhance reciprocal sharing on known and suspected threats.	Minister of Public Safety, Minister of Canadian Heritage **Joint activities:** • Protecting Canada's Democracy MC approved at 17 May Full Cabinet
C.	(Bolstering Security and Defence, 40, Building Back Better 15)	Minister of Natural Resources **Joint activities:**

Current as of 17 June

	Deliverables: (40) Implement a Framework for Collaboration on Cybersecurity in the Energy Sector to enhance security and resiliency of cross-border energy infrastructure. (15) Renew and update the existing MOU on energy between the US DOE and NRCan.	• Text of NRCan–DOE MOU finalized; Ministerial bilat and signing taking place possibly as early as June 24 or June 25 • Canadian priorities for collaboration under Framework proposed during meeting of US Energy Government Coordinating Council meeting on June 3 (Threat assessment, preparedness exercises, R&D); US DOE response pending.
D.	(Bolstering Security and Defence, 35) **Deliverable:** Expand cooperation on continental defence/defence and in the Arctic, including by modernizing the NORAD Defence Command.	Minister of National Defence, Minister of Foreign Affairs **Joint activities:** • DND decks on NORAD/Continental Defence moving through June CGAPS • US-Canada Arctic Dialogue targeting Late-Summer/Early-Fall; Arctic Governance and Security anticipated to be agenda items, as per US Directors Group update • Late-Summer/Early-Fall target for 2+2 Ministerial Meeting; agenda anticipated to be light on Continental Defence, heavy on global regional security hot spots
E.	(Building Back Better, 13) **Deliverable:** Strengthen Canada-U.S. supply chain security and reinforce deeply interconnected and mutually beneficial economic relationship.	Minister of Small Business, Export Development and International Trade, Minister of Innovation, Science and Industry **Joint activities:** • Discussion of cyber security certification and standards scheduled for DMCS 24 June, including specific reference to US approach of Cybersecurity Maturity Model Certification for Defence Industrial Base

4. Key Messages:

- Ransomware as a priority issue for both Canada and the United States government. This persistent threat ties together issues of critical infrastructure and supply chain security, criminal investigation and law enforcement, and, cryptocurrency and money laundering.

- There is opportunity for Canada and the US to work together on understanding, preventing, defending against and recovering from ransomware incidents, including through information sharing, joint exercises, and communications to partners in industry, other levels of government and critical infrastructure.

Current as of 17 June

- Whereas the US has announced the intention to regulate cyber security for critical infrastructure, Canada has been close to tabling legislation on Critical Cyber Systems which would achieve a similar goal.

- Supply chain security and country agnostic efforts to 'raise the cyber security bar' are ongoing for both countries and efforts to communicate best practices so that every citizen can play a role in cyber security remain important.

Public Safety Canada | Sécurité publique Canada

BUILDING A **SAFE** AND **RESILIENT** CANADA

Canada-United States Engagement on Ransomware

June 24, 2021
RDIMS # 3963810

Canada

Cyber Security a Joint Priority

BUILDING A SAFE AND RESILIENT CANADA

- The Covid-19 pandemic has increased our reliance on digital services.
- Accordingly, cyber security is a priority of the Government of Canada (GC) and is a top priority for the Biden administration.
- Due to the transnational nature of cyber threats, collaboration is imperative. We must take a proactive and engaged approach to maximize the effectiveness of our efforts against ransomware.
- In February 2021, Canada and the United States (U.S.) included cyber security as a key component of the "Roadmap for a Renewed U.S.-Canada Partnership."
- It is recommended that ransomware be singled out as a priority for bilateral action on cyber.

Why Ransomware?

- Flourishing criminal industry that threatens the personal and financial security of individuals as well as national security and human life.
- Cyber Centre assessed that cybercriminals are adopting more sophisticated tactics, targeting critical organizations and their suppliers, escalating ransom demands, and are increasingly linked to state actors.
- Severity of recent ransomware incidents:
  - Colonial Pipeline
  - JBS Meatpacking
- US Secretary of Homeland Security Alejandro Mayorkas identified ransomware as a national security threat; US Department of Justice is prioritizing and centralizing ransomware incidents in a manner similar to terrorism cases.

Proposed Areas of Collaboration

BUILDING A SAFE AND RESILIENT CANADA

- Cyber Insurance
- Outreach and Engagement Approaches (to improve cyber resilience)
- Crypto Currency
- Anti-Money Laundering and Terrorist Financing
- Incident Response (including walkthroughs or table top exercises; identifying legislative gaps on incident response mandates)
- Cyber Operations and Law Enforcement Actions (to disrupt cyber criminals)
- International Engagement

Next Steps

- Seek DM endorsement of ransomware as our cyber priority in bilateral work with U.S. counterparts.
-
-
- Given the evolving nature of the threat, additional areas of Canada-U.S. collaboration on ransomware may be identified and added to the action plan.

Public Safety Canada | Sécurité publique Canada

BUILDING A **SAFE** AND **RESILIENT** CANADA

Cyber Security Certification

24 June 2021

RDIMS # 3915918

Canada

Cyber Security Certification – Background

BUILDING A SAFE AND RESILIENT CANADA

- Cyber certification of a company provides assurances that the company meets a designated standard for cyber security, mitigating risks for issues like supply chains, information loss, third party vulnerabilities, etc.

- ISED leads CyberSecure Canada, a certification program for Small and Medium Enterprises.

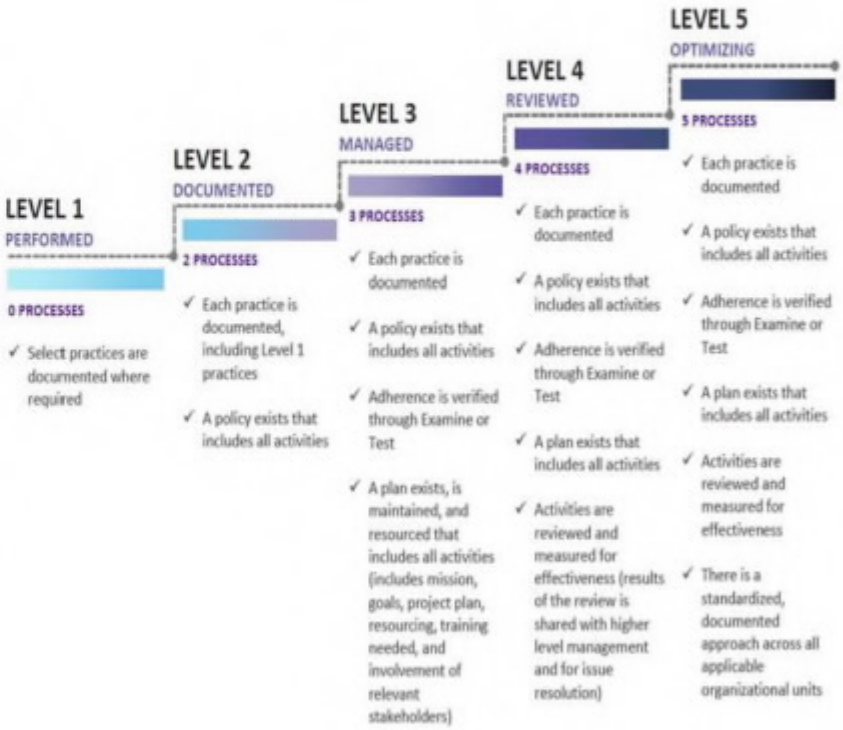
- The US Department of Defense has introduced the Cybersecurity Maturity Model Certification Program for contractors, creating challenges for Canadian based defence and security companies.

- Currently, Government of Canada contracts do not have stipulations for cyber security certification outside of classified systems.

US Cybersecurity Maturity Model Certification

BUILDING A SAFE AND RESILIENT CANADA

- Protects "Controlled Unclassified Information" in US Department of Defense supply chains; requirements are based on an ensemble of existing standards
- Scalable to five levels of certification based on the level of sensitivity or criticality of the information.
- Administered by a non-profit accreditation body; audits carried out by Certified Third-Party Assessment Organizations (C3PAOs)



Public Safety Canada | Sécurité publique Canada

CMMC and Canada

BUILDING A SAFE AND RESILIENT CANADA

- A reciprocal Canadian program could:
  - enhance and verify supply chain resiliency

- There is no existing Canadian cybersecurity standards program that matches CMMC requirements
  - CyberSecure Canada may be only partially reciprocal with CMMC Level 1
- The US has acknowledged that other countries can adopt CMMC or seek reciprocity, but there is not yet a process for allowing US assessors into Canadian companies for certification **or** for certifying Canadian auditors

Beyond the Defence Sector

BUILDING A SAFE AND RESILIENT CANADA

- Certification is important for all sectors, not just Defence
- Along with standards, certification is a key part of supply chain security
  - International fora, such as the [redacted] and the G7, have identified the need for resilient and reliable supply chains in various sectors, including telecommunications
- With the dramatic increase of internet-connected devices in sectors like transportation and health, cyber security certification would play an important role in the safety and security of Canadians
- [redacted]
- Canada continues to develop standards in collaboration with allies and partners, but certification remains a gap

Policy Decisions

BUILDING A SAFE AND RESILIENT CANADA

- Is a Canadian certification program needed? If so, what is the **scope**?

- Who is the **lead department**? What are the roles of supporting departments?

- Proposed next steps

Public Safety Canada | Sécurité publique Canada

Mid-Term Review of the National Cyber Security Strategy

(For DMCS information)

ISSUE

In Spring 2021, Public Safety Canada launched the Mid-Term Review of the National Cyber Security Strategy (NCSS) to evaluate early returns from investments and ensure the Strategy remains relevant and responsive to an evolving cyber security landscape.

The Review is being led by Public Safety Canada, in consultation with NCSS signatories and the broader federal cyber security community.

SCOPE OF THE REVIEW

The Review is examining the relevance, performance, and impacts of the Strategy, including the 14 NCSS horizontal initiatives. Objectives are to:

1. Review progress made toward expected outcomes in the first 3 years of NCSS implementation;
2. Assess the continued relevance of the Strategy in our current environment;
3. Identify gaps and opportunities for near- and mid-term refinement, and;
4. Lay the foundation for other policy work to be completed in preparation for 2024.

Public Safety is expected to report back to NCSS signatory Ministers on the outcomes of the Review in Spring 2022. To note, federal partners are leading related initiatives in parallel to this work, including the National Critical Infrastructure Strategy Renewal, the Review of the C59 Act, and the 3-year Review of the Canadian Centre for Cyber Security. Public Safety is working with other federal leads to align the activities and insights that emanate from these reviews.

STATUS

An interdepartmental Tiger Team led by Public Safety is currently engaging in consultation activities internal to the federal cyber security community to gather information and insights to support the review process. A literature review, international benchmarking exercise and environmental scan are being conducted in parallel to this work.

Departments contributing to the Tiger Team's efforts are: Communications Security Establishment (CSE), Canadian Security Intelligence Service (CSIS), Royal Canadian Mounted Police (RCMP), Global Affairs Canada (GAC), Innovation, Science, and Economic Development (ISED), Public Safety Canada (PS), Natural Resources Canada (NRCan), Employment and Social Development Canada (ESDC), Transport Canada (TC), Department of National Defence/Canadian Armed Forces (DND/CAF), Privy Council Office (PCO), Justice Canada, and Health Canada (HC).

TIMELINES

- **Launch Mid-Term Review** (March 2021)
  - Strike Interdepartmental Tiger Team

Public Safety Canada | Sécurité publique Canada

- **Information-Gathering and Analysis Phase** (Spring-Summer 2021):
  - Internal Consultation and Engagement Activities
  - Mid-Term Evaluations of NCSS Programs and Initiatives
  - Environmental Scan
  - Literature Review
  - International Benchmarking
  - Identification of Gaps and Improvement Measures
- **Reporting Phase**
  - Interim Report to DGCS: Fall 2021
  - Preparation of Draft and Final Report: Fall 2021
  - Endorsement of Final Report by Cyber Security Committees: Fall 2021-Winter 2022
  - Presentation of Final Report to Ministers: Spring 2022

CADSI

DEFENDING OUR FUTURE. **TOGETHER.**

Towards a cybersecurity standard for Canadian defence procurements: effective, secure, and recognized

This note sets out CADSI's views to inform the development of a potential Canadian cybersecurity standard used in Canadian defence procurements and throughout relevant defence supply chains. This is based on consultation with CADSI members. CADSI is willing to present to the relevant government committees discussing this issue.

Thought is given as well as to how the Government of Canada (GC) might respond to the U.S. Department of Defense (U.S. DoD) Cybersecurity Maturity Model Certification (CMMC). A cyber standard for controlled unclassified information (CUI) is a new industrial risk not yet covered by existing Canada-U.S. industrial security agreements or the Controlled Goods Program's (CGP) current mandate. Regardless of which path GC chooses, either a unique Canadian cybersecurity standard or adopting CMMC by reference, it will need to respond to the U.S. CMMC requirements and seek reciprocity to maintain Canadian market access to the U.S.

The key elements of CADSI's views are:

1. Companies should be independently verified, as opposed self-assessed, against the standard.
2. The GC should adopt U.S. DoD's CMMC by reference for use in Canada, thereby making it a binational standard that could become the basis for a Five-Eyes wide standard.
3. The GC should secure, for Canadian firms, non-discriminatory access to those services offered to U.S. firms under the auspices of the existing U.S.-based CMMC Accreditation Body (CMMC AB).
4. One GC organization should manage delivery of all aspects of an industrial security program (i.e. personnel, facility, and cyber).

General Comments:

A collaboratively developed and implemented cybersecurity standard for Canada would improve the cyber security posture of Canada's Defence Industrial Base (DIB), just as screening individuals and securing facilities has done.

- The cybersecurity standard for Canada should be internationally recognized, independently verified, reciprocal with our closest allies (e.g. Five Eyes) and impose minimal burdens on Canadian firms.
- The U.S. Government (USG) is setting cyber security standards that will likely be adopted by other countries. If Canada does not keep pace, Canadian companies may face market assess and non-tariff trade barriers in competing for their procurements. Cyber security standards could be used by U.S. primes and incumbent suppliers as a point of leverage against foreign firms seeking to access those U.S. supply chains, similar to how DoD has used ITARs to exclude foreign firms.
- An establishment of an effective and efficient standard should be seen and developed not only to render the Canadian DIB more secure, but also to contribute to its competitiveness and retain, if not, expand its market access as a trusted partner with the U.S. and other key allies.
- While the cybersecurity standard for Canada should be mandatory, Canadian firms may request assistance and incentives to make the required financial investments and business process changes. As 90% of Canadian defence companies are SMEs, their financial capacity to implement

300-251 Laurier Avenue West
Ottawa, ON K1P 5J6
defenceandsecurity.ca

T: +1 613.235.5337
F: +1 613.235.0784
cadsi@defenceandsecurity.ca

a standard quickly and effectively might be challenged. Consideration should be given to how the government can support the implementation of a cybersecurity standard for Canada. This could include ITB credits and the use of multipliers, tax code measures such as accelerated depreciation, Regional Development Agency grants, and technical assistance from the Canadian Centre for Cyber Security (CCCS).

- Many countries are appealing to non-traditional suppliers to support their defence departments and militaries. For companies who have very little or no experience operating in a managed defence market, commercially focused companies often judge the complexity and compliance costs as too high to service the market. The GC should explore ways to make facilitate these firms to join the DIB, thereby expanding its base of potential suppliers.

Standards Related Comments:

Canadian industry strongly prefers adopting the U.S. DoD's CMMC by reference for use in Canada.

- The cybersecurity standard for Canada applied in Canada will need to address concerns of both the Canadian and U.S. governments, as well as reflect current and evolving marketplace practices and dynamics. The data in question will be subject to both frameworks given how companies integrate U.S. and Canadian data, which are subject to both ITAR and Controlled Goods, in practice.
- The U.S. has already rolled out CMMC, and it is emerging as a recognised standard. Having a common standard can help Canadian defence firms earn and maintain the "digital trust" of their customers and compete globally. It will also help firms remain aligned with increasing U.S. export controls and security of supply regimes than would a separate Canadian standard.
- Canadian companies are highly motivated to comply with CMMC – as is – so they can continue to do business directly with DoD and participate in U.S. supply chains and Canadian subsidiaries of U.S. firms. ISED's existing CyberSecure Canada is a general marketplace standard, not a suitable standard for defence companies that face more sophisticated and determined cyber adversaries.
- Having a separate Canadian standard would apply additional burdens on Canadian firms. First, Canadian companies would need comply with two evolving standards that will change over time, unlike their U.S. competitors. Secondly, Canadian companies would need to explain to risk adverse American procurement officials why and how a separate Canadian standard is synonymous with CMMC (with or without a reciprocal agreement), a cost and risk U.S. firms would avoid. This dynamic is already at play on ITAR-security related concerns.
- CMMC will also impact domestic Canadian defence procurements. U.S. primes and their Canadian subsidiaries bidding on Canadian defence procurements will be more inclined to include Canadian firms in their supply chains that are U.S. DoD CMMC compliant. This provides greater confidence for U.S. primes that their Canadian suppliers can be used interchangeably for products also destined for the U.S. and other global markets. U.S. primes will see replacing non-CMMC standard products as a cost.
- The GC has not provided industry with a convincing rationale as to why a unique Canadian standard is warranted and how the benefits outweigh the costs. If both Canadian and U.S. defence contractors are facing the same adversaries, CADSI does not see how this warrants a separate Canadian cybersecurity standard.
- The flow down requirements of a standard for Canada into a supply chain could provide large foreign primes bidding on Canadian procurements with more leverage and opportunities than smaller Canadian firms to pass on Canadian-only compliance costs to the Government of Canada. This disadvantages Canadian SMEs.

Implementation Related comments:

Canadian industry strongly prefers having one government organization manage delivery of all aspects of an industrial security program (i.e. personnel, facility, and cyber).

- In its discussions, the GC should focus as much, if not more, on how the standard is effectively and efficiently implemented, not solely on what that standard is.
- The program should be properly resourced, and the regulator should have a general knowledge of the marketplace, current dynamics, and practices, how the technologies interact with the compliance framework, and how these factors translate into risks to Canadian national security.
- The GC has told industry that PSPC's Industrial Security Program, part of the Oversight Branch, is the GC's industrial security program of record, responsible for administering Canada's industrial security programs and for managing international industrial security agreements. This program has established infrastructure, relationships, communications channels, and a community of interest. It already works to protect industrial personnel and places through the Contract Security Program and the Controlled Goods Program. The CGP already undertakes verified, physical inspection of some company IT systems within its existing mandate.
- Cyber security risks cannot be separated from personnel risks, in practice, so separating the government organizations responsible for each threat vector is not effective.
- GC will need to negotiate an update its bilateral industrial security agreement with the USG to addresses cyber CUI information.
- At a minimum, Canadian firms need to have access to services offered under the auspices of the CMMC AB – services which are not exempt from trade treaties. If possible, Canadian firms should be allowed to offer these services by undergoing the same requirements as U.S. firms.
- Two other considerations are: (i) how DND's cyber mission assurance standard (SSE #87) will interface with a cybersecurity standard for Canada; and (ii) how the standard will handle threat monitoring and sharing capability between Canadian defence companies and GC, a function required under CMMC for high trust suppliers. Threat data, when aggregated across the Canadian DIB, has significant value for Canada, and it should not be unreservedly given away, as is called for under U.S. DFARS.

Contact

For more information, please contact:

Nicolas Todd
Vice President, Government Relations and Communications
Canadian Association of Defence and Security Industries (CADSI)
nicolas@defenceandsecurity.ca / Tel: 613.235.5337, ext. 37
251 Laurier Avenue West, Suite 300, Ottawa, ON K1P 5J6
www.defenceandsecurity.ca

V: 27 May 2021