National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

Cyber Security Program Certifications for the Canadian Defence Supply Chain

Lieutenant-Colonel Gina Decarie

JCSP 48

Exercise Solo Flight

Disclaimer

Opinions expressed remain those of the author and do not represent Department of National Defence or Canadian Forces policy. This paper may not be used without written permission.

PCEMI 48

Exercice Solo Flight

Avertissement

Les opinons exprimées n'engagent que leurs auteurs et ne reflètent aucunement des politiques du Ministère de la Défense nationale ou des Forces canadiennes. Ce papier ne peut être reproduit sans autorisation écrite.

Canada

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES

JCSP 48 – PCEMI 48
2021 – 2022

Exercise Solo Flight – Exercice Solo Flight

Cyber Security Program Certifications for the Canadian Defence Supply Chain

Lieutenant-Colonel Gina Decarie

THE WEAKEST LINK: EVALUATING CYBER SECURITY PROGRAM CERTIFICATIONS FOR THE CANADIAN DEFENCE SUPPLY CHAIN

INTRODUCTION

The sustainment and equipping of the Department of National Defence (DND) such that DND is able to meet its objectives is no small challenge. Aside from the internal Canadian Armed Forces (CAF) and DND offices that conduct sustainment, many other government departments are also involved. These include Public Services and Procurement Canada (PSPC) which is Canada's central purchasing agent, and Innovation, Science, and Economic Development (ISED) Canada that engages and consults with industry stakeholders to ensure that Canada's needs are met while also promoting and protecting Canadian industry. DND, PSPC, and ISED have key roles in ensuring that DND receives the equipment and capabilities it requires, that national security concerns related to procurement are respected, and that Canadian economic development is supported. A fourth governmental department, the Communications Security Establishment (CSE), provides technical advice and holds authorities related to cyber security. CSE is an essential department for some procurements relating to information sharing, as area of significant and increasing concern within defence procurement circles.

Information sharing is vital if DND is to be properly sustained. At the same time, sharing too much information, even unclassified, could result in adversaries obtaining an unacceptable level of knowledge about CAF operations that could put national security at risk. To further complicate matters, interoperability within coalitions such as the North American Aerospace Defense Command (NORAD) and the North Atlantic Treaty Organization (NATO) requires that defence information be sometimes shared with

vendors, suppliers, and contractors who are not Canadian. This can create challenges if the contractors have not been screened, or if the products they sell have inherent vulnerabilities that are not in either the vendors' interests to divulge or in Canada's best interests to implement. Similarly, the means through which information is shared, even amongst trusted partners, is equally vulnerable to a cyber attack.

When Canada's Defence Policy, *Strong, Secured and Engaged (SSE)*, was published in 2017, it explicitly recognized the risks to CAF sustainment in Initiative 87: "protect critical military networks and equipment from cyber attack by establishing a new Cyber Mission Assurance Program that will incorporate cyber security requirements into the procurement process."[1] As a result of SSE Initiative 87, the Assistant Deputy Minister Materiel (ADM (Mat)) was tasked to examine the CAF's supply chain for platform systems, which are vehicles or structures that may host weapons systems, and develop a program that addresses cyber security vulnerabilities. ADM(Mat) then began to consider similar programs that already exist in both the United States (US) and the United Kingdom (UK).[2]

Given the requirement to share defence information and the related cyber security risks, this paper asks the following question: are policies and programs in place for cyber security in the defence supply chain in either the US and UK suitable for implementation in Canada? This question will be answered by first addressing the national security concerns emanating from information sharing in the defence procurement system and in

[1] Department of National Defence, *Strong, Secure, Engaged: Canada's Defence Policy* (Ottawa: Canada Communication Group, 2017), 73.

[2] Department of National Defence, "Supply Chain Risk Management: Initiatives at Department of National Defence, Brief to CIPMM Virtual Summit," 3 June 2021, slide 3.

particular, discuss the policies that govern how information is currently shared and stored. Recognizing that shortfalls remain in the way in which the latter is handled in Canada, the paper will then examine both the US and UK information sharing, processing and storing policies to see if they can be adapted for Canada's use. At issue also is the matter of data sovereignty as it pertains to national security when working alongside coalitions, and the paper, while addressing this issue, will finally suggest how Canada's domestic procurement policies can be safeguarded in such situations with a view to protect sensitive information during a procurement process.

INFORMATION SHARING IN WARFARE

The transmission of sensitive information used for a competitive edge against an adversary has been in existence as long as warfare. This type of transmission was perhaps first organized in modern warfare terms by the Chappe system in the late 18th century and later expanded by Napoleon Bonaparte. The Chappe system relied on predetermined codes in order to transmit information over a long distance using directed light signals and this system was the first in modern times to outpace a horse in terms of transmission speed.[3] From this rudimentary system, through the telegraph, radio, the telephone, and many iterations of telecommunications improvements, military practitioners have honed their capabilities to send and receive information, as well as the ability to prevent their adversaries from receiving the same information.

The protection of friendly information while denying the same to adversaries is a basic principle of operational security, and as military campaigns evolved over time, such

[3] John Olsen and Martin van Creveld, *The Evolution of Operational Art: From Napoleon to the Present* (Oxford: Oxford University Press, 2011): 16-17.

that war fighting took place further from the strategic headquarters, increasing amounts of data sent over a long distance began to require increasing levels of protection against interception and interpretation. The exponential pace of information technological advancement from the late 1700s to the early 21st century meant that protecting sensitive military data has evolved from simple point-to-point directed light codes to advanced cryptographic digital signals sent across multiple nodes. The protection of sensitive information has taken on various forms over the intervening years between the Chappe system and today, but the foundation of information security ensures that information remains only in the hands of those who need it (confidentiality), remains intact and not tampered with (integrity), and accessible to those who need it (availability). The confidentiality, integrity, and availability triad is known as CIA, and modern information security professionals use this triad as a guiding framework when assessing whether information is 'secure.'[4]

Information sharing in the modern sense tends to be conflated with various contemporary domains: personal information, digital identity, intellectual property, and national security, among others. All of these domains have aspects of information security but different approaches in application to the CIA triad. For individuals, the protection of personal information has various implications, from the risk of release of potentially embarrassing information to the risk of identity theft that has far-reaching implications. For companies, the protection of intellectual property is of increasing importance, as the 'intellectualization' of goods and services experiences an upward

[4] Josh Fruhlinger, "The CIA triad: Definition, components and examples," last modified 10 February 2020, https://www.csoonline.com/article/3519908/the-cia-triad-definition-components-and-examples.html.

trend.[5] Recent state-sponsored attacks on US industry from Russia and China have illustrated the dangers of intellectual property theft, and a Japanese survey in 2018 revealed that a quarter of all successful cyber attacks in that country were for the purposes of stealing intellectual property.[6]

In terms of national security, there are three main factors to consider for CIA: information sharing within one's own forces, information sharing within alliances, and information denial for adversaries. Arguably, information sharing within one's own forces can be procedurally easy: national security classifications dictate the level to which information can be shared according to a national security clearance and within a 'need to know.' Information denial is likewise relatively simple in principle: deny all those who would leverage sensitive information against you from obtaining such information. In practice, the application of these basic principles is subject to the skill and technological tools at one's disposal. Further discussion on information sharing within one's own forces and information denial is outside the scope of this paper.

The third category of CIA consideration - information sharing with alliances - can be complicated. Alliances are not only those similar forces with which one might partner, but can also include academic, industrial, commercial, and other government departments that wish to partner with defence organizations for various reasons. These entities may or

---

[5] Vladlena Lisenco, "Improving the practice of Competitive Strategies for the protection of Intellectual Property: the law and economics approach," *Eastern European Journal of Regional Studies* 7, no. 1 (June 2021): 173-176.

[6] White House Office of Trade and Manufacturing Policy, *How China's Economic Aggression Threatens the Technologies and Intellectual Property of the United States and the World*, (Washington, DC: U.S. Government Printing Office, June 2018), 3.

may not have security clearances, be economically beholden to adversaries, or seek financial gain from defence vulnerabilities.

CANADIAN DEFENCE PROCUREMENT

When the Department of National Defence (DND) identifies requirements for capabilities one of two things typically happens. Either the department seeks a sole source contract with a company that is known to be the only one able to provide a mature product or service, or the requirement is codified in a Request for Proposal and industry is provided the opportunity to bid on fulfilling the requirement. In the former case, DND selects a contractor and industry provides the well-defined product or service. In the latter, however, a delicate iterative balance is sometimes required. DND may recognize that an operational deficiency exists, but departmental experts may not be positioned to know what is available from industry that best resolves the deficiency. Therefore, some information sharing from DND to potential commercial providers, and vice versa, may be required to ensure that DND contracts a solution that best fits the requirement. This type of shared information is typically unclassified but if agglomerated could provide a picture of DND's capabilities that would be considered classified.

DATA SOVEREIGNTY

All data on the open Internet today exists within a data ecosystem, which at a minimum includes the user, the Internet Service Provider (ISP), and providers such as a website, a streaming service, or an Internet-enabled application. Data sovereignty refers to individuals or organizations' autonomous ability to control where their information is

being transmitted or stored by a cloud service provider.[7] In a 2020 White Paper, the Treasury Board of Canada Secretariat noted that loss of data sovereignty could damage the Government of Canada's interests if sensitive information stored outside of Canada is subject to that country's laws and disclosed without notice.[8] The concept of data sovereignty, like CIA, means different things depending on the application. For individuals, data sovereignty is the personal right to direct who is allowed to hold specific data, such as financial information, social insurance numbers, health records, and digital markers like browser cookies and search histories. This right is treated differently in different countries, and Canada has enacted several laws that relate to personal data sovereignty on the Internet.[9] Perhaps the most relevant to the concept of deciding what and when to share data, and to who, is the use of cookies and more specifically, third-party cookies.

Cookies, tiny bits of text embedded in a web browser, allow analysts to track what sites users visit, how long they stay, where they navigate to and from the site, their location, and what type of device they are using. There are more second-order metrics that could be gleaned from this information, such as an extrapolation of the user's age, location, gender expression, family status, and occupation.[10] Cookies are normally collected by the host website to aid the user in navigating a page and restoring their last

---

[7] Matthais Jarke, Boris Otto, and Sudha Ram, "Data Sovereignty and Data Space Ecosystems," *Business & Information Systems Engineering* 61, no. 5 (October 2019): 549-550.

[8] Treasury Board of Canada Secretariat, "Government of Canada White Paper: Data Sovereignty and Public Cloud," last accessed 3 May 2022, https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/gc-white-paper-data-sovereignty-public-cloud.html.

[9] Parliament of Canada, "An Act to amend the Personal Information Protection and Electronic Documents Act and to make a consequential amendment to another Act," last accessed 3 May 2022, https://www.parl.ca/LegisInfo/en/bill/41-2/S-4.

[10] T. Eggendorfer, "Using third party cookies for forensic identification," *Proceedings of the International Conference on Security and Management (SAM), Athens* (2015): 16-22.

visit. Third-party cookies, however, are bits of code embedded on the host website by another company that pays for access to this information. Due to the vast amount of data that this type of collection accumulates, as well as various privacy laws, personal information is often stripped from the data collected such that it is anonymous.[11] Even without the use of cookies, tiny files called beacons track user information in a similar manner to cookies and are often embedded in e-mails and web pages.[12]

The problems with this type of data agglomeration, even if the data is anonymized, are twofold. First, users are not necessarily aware of the amount of information that is being scraped from their online activity. A simple search engine entry combined with a particular selection of presented links has meaning for present-day big data consumers and resellers. That is to say, the free web searching services delivered by Bing and Google, for example, are free because they can correlate large amounts of web activity and sell premium advertising placements based on user history using online tracking tools.[13] The sale of this information, vis-à-vis the online behaviour of an individual user, is not transparent to the average user, and this loss of privacy is frequently accompanied by a loss of data sovereignty. Second, because all the information and data related to a users' virtual activity can now be assembled, collated, and analyzed, the concept of being anonymous on the web is gone, unless the user undertakes significant and deliberate efforts to remain so. Despite the data being

---

[11] *Ibid.*

[12] Office of the Privacy Commission of Canada, "Frequently asked questions about cookies," last accessed 19 April 2022, https://www.priv.gc.ca/en/privacy-topics/technology/online-privacy-tracking-cookies/cookies/frequently-asked-questions-about-cookies/.

[13] Google Ads, "Reach new customers online with Google Ads," last accessed 3 May 2022, https://ads.google.com/home/?utm_source=marketingplatform.google.com&utm_medium=et&utm_campaign=marketingplatform.google.com%2Fabout%2Fresources%2Fanalytics-data-controls-feature-brief%2F.

anonymized, the sheer amount of data available means that clever filtering and searching can quickly identify an individual based on limited known parameters.[14]

Looking now at data sovereignty from a defence industrial complex perspective, parallels to personal data can be drawn. Certainly large defence supply chain providers tend to have the resources to apply to cyber security, should they deem it a priority. These larger companies have the resources to safeguard company information in ways that average individuals do not for their personal information, such as teams of information technology (IT) professionals who can monitor network activity in search of unauthorized data gathering. Not all companies, however, have these resources or have made cyber security a priority. These companies would therefore be at the same mercies as the average individual – that is to say, vulnerable to data scraping from those who would profit from obtaining information related to national security. Similar to personal data pilferage from the average Internet user, companies without adequate cyber security safeguards can lose information through both direct cyber attacks and data scraping through access by opportunity as a result of lax security. In the worst case, information loss can include Controlled Unclassified Information (CUI) residing within a company in Canada's defence supply chain and DND has thus lost data sovereignty over sensitive information. In order to prevent the loss of CUI in the supply chain, a control system should be implemented that safeguards national security while respecting the vendors' technical abilities. The US and the UK have implemented such systems in recent years

[14] Michael Trusov, Liye Ma and Zainab Jamal, "Crumbs of the Cookie: User Profiling in Customer-Base Analysis and Behavioral Targeting," *Marketing Science* 35, no.3. (May-June 2016): 405-426.

and DND must recommend to the Government of Canada if either of their models are implementable in Canada or if a modified version is required.

ALLIES' APPROACHES

> *"…cyber crime and the resulting loss of our intellectual property and technology to our competitors [is] 'the greatest transfer of wealth in U.S. history'"*
>
> *-Former director of the National Security Agency, General Keith Alexander*

The US introduced the Cyber Maturity Model Certification (CMMC) in 2019 as a means to certify the cybersecurity practices of contractors, with varying levels of compliance requirements depending on the type of information that they access.[15] The CMMC integrates and supersedes previous federal compliance requirements for the treatment of CUI, using the US National Institute of Standards and Technology (NIST)'s publication SP 800-171, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations," which addresses "protecting controlled unclassified information in non-federal systems and organizations."[16]

There are three tiers to the latest version of the CMMC. Tier 1 is the 'foundational tier' for contractors with access to the lowest level of sensitive information and certification for this tier is achieved by maintaining 17 cybersecurity practices that are verified annually through self-assessment. Tier 2, the 'advanced' tier demands 110 cybersecurity practices that are aligned with NIST SP 800-171, and verification is

---

[15] Aleksey House, "The Price of a Cybersecurity Culture: How the CMMC Should Secure the Department of Defense's Supply Chain Without Harming Small Businesses and Competition," *Public Contract Law Journal* 50, no. 3 (Spring 2021): 449-470.

[16] Acquisition and Sustainment, Office of the Undersecretary of Defense, "About CMMC," last accessed 6 April 2022, https://www.acq.osd.mil/cmmc/about-us.html.

completed thrice annually by third-party assessors. Finally, Tier 3, the 'expert' tier requires more than 110 of these practices and verification is done thrice annually through government-led assessments.[17] Despite being designed with allies' reciprocity in mind, this program is aimed primarily at US suppliers; the CMMC Accreditation Body certifies only US Certified Third Party Organizations (C3PAO), thus any Canadian accreditor for Canadian companies cannot be CMMC-compliant. As such, a major challenge to this program from the Canadian perspective is that suppliers wishing to be included in the US CMMC program would first be subject to review by US assessors. This raises sovereignty concerns with foreign assessors having access to Canadian CUI.[18]

The UK has also implemented a national program meant to safeguard sensitive Ministry of Defence identifiable information (MODII) by working with supply chain partners through the Defence Cyber Protection Partnership (DCPP) Cyber Security Model (CSM), which came into effect in October, 2017.[19] The CSM requires a procurement Authority to identify whether the procurement requires the sharing of MODII and if so, to assign the procurement as falling into one four categories: Very Low, Low, Moderate, and High. This Authority assessment produces a Risk Assessment Reference that potential suppliers can use to confirm whether they are capable of compliance to the security standards that the MODII in question requires.[20] Risk Assessments are assigned a level, depending on the level of sensitivity of the MODII. In

[17] *Ibid.*

[18] Assistant Deputy Minister (Materiel), "Cybersecurity Maturity Model Certification (CMMC) and Canada, ADM Cyber Security Committee," May 2021, slide 6.

[19] Defence Cyber Protection Partnership, *Defence Cyber Protection Partnership Cyber Security Model Industry Buyer and Supplier Guide*, (Kew: The National Archives, June 2018), 1.

[20] *Ibid*, 1-5.

order for a supplier to compete for contracts, the higher the sensitivity level of the MODII, the higher the certification the potential supplier requires.

The UK CSM uses ISO 27001 for certifying whether a supplier is compliant with cyber security deemed required by the Ministry of Defence (MoD) Authority. ISO 27001 outlines the IT, security techniques, and information security management systems requirements that are deemed applicable to any organization, regardless of type, size, or nature.[21] In order to monitor supplier compliance with this standard, the MoD, in partnership with the UK National Cyber Security Centre, has a contract with Information Assurance for Small and Medium Enterprises Consortium (IASME), a not-for-profit organization. IASME offers both the Cyber Security Essentials certification, which is a self-assessment tool, as well as the Cyber Essentials Plus certification, which provides similar assessment tools as the basic certification but conducted by a qualified assessor rather than relying on self-assessment.[22] Only assessors based in the UK or in Crown Dependencies may be registered assessors for the UK CSM.[23]

The US CMMC program is similar to the UK CSM in four key aspects. First, a responsible defence procurement authority is required to designate whether the procurement project or program requires sharing of sensitive, unclassified information. Second, both security programs require vendors to have a minimum certification related to cyber security practices and as the level of sensitivity increases, so do the vendor

[21] ISO, "ISO/IEC 27001:2013," last accessed 21 April 2022, https://www.iso.org/standard/54534.html.

[22] IASME Consortium, "Cyber Essentials; The Benefits of Certification," last accessed 21 April 2022, https://iasme.co.uk/cyber-essentials/.

[23] IASME Consortium, "Become an Assessor," last accessed 21 April 2022, https://iasme.co.uk/become-an-assessor/#:~:text=To%20become%20an%20IASME%20Governance%20Assessor%2C%20you%20will%20first%20need,CISM.

certifications and levels of scrutiny and oversight. Third, the defence organization has delegated basic vendor certification to a third party: the C3PAO program via the CMMC Accreditation Body for the US and IASME for the UK. Finally, both programs are specific to their country of origin: only US-based assessors can certify a vendor as CMMC-compliant, and only a UK or Crown Dependency-based assessor can certify a vendor as CSM-compliant. In contrast between the US and the UK model, the UK has also implemented the Defence Assurance Risk Tool (DART), which registers Information and Communications Technology (ICT) systems that hold, process, or store MOD data.[24] This additional level of certification means that vendors who wish to compete for MOD contracts must use a DART-registered system to store or process MODII, unless the MODII category has been categorized as 'Very Low.'

Some details of the US and the UK models leave Canada in a quandary when it comes to adopting either model as-is. The US model is based on the US' own NIST publication, while the UK model is based on an international ISO standard. The US model is more open to any vendor that can prove its cyber security hygiene, while the UK model is more prescriptive on using registered ICT providers. The use of registered ICT providers for MODII may help UK security agencies to focus their active defensive efforts against adversaries attempting to scrape information from vendors. In the US however, all data routed through US nodes is open to surveillance by the National Security Agency (NSA). The NSA's mass surveillance capability may be what enables

[24] Ministry of Defence, "Industry Security Notice Number 2017/01," last accessed 29 April 2022, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/594320/DART_ISN_-_V2_3.pdf

US vendors to use any ICT of choice, since all data is actively monitored.[25] Both the US and UK models have their advantages and disadvantages for use in Canada's defence supply chain, and both offer different perspectives on how to advantage domestic economic interests, a topic to which the paper turns next.

THE CANADIAN APPROACH TO DATE

Innovation, Science, and Economic Development (ISED) Canada champions, among other files, Canada's small and medium enterprise (SME) economic success domestically and abroad. There are two main ISED initiatives that address cyber security and SME. The first is the Cyber Security Innovation Network, an initiative that aims to connect innovators in the private sector to those in academia and the public sector so that advances in the cyber security field can be shared and instituted. The second is CyberSecure Canada, an initiative that leverages best practices developed by CSE and certifies SMEs through independent audit on the implementation of these practices.[26] Similar to the US model, several companies are registered as accredited certification bodies for CyberSecure Canada, but unlike the US or UK that rely on a contracted third party, only a government entity – the Standards Council of Canada – can accredit the certification bodies.[27]

In addition to domestic initiatives, Canada is actively involved in working groups at the United Nations (UN) and NATO. The United Nations General Assembly resolution

---

[25] Dan Breznitz, "Data and the Future of Growth: The Need for Strategic Data Policy," last modified 19 April 2018, https://www.cigionline.org/articles/canadian-network-sovereignty/.

[26] Canadian Centre for Cyber Security, "Baseline cyber security controls for small and medium organizations," last accessed 22 April 2022, https://cyber.gc.ca/en/guidance/baseline-cyber-security-controls-small-and-medium-organizations.

[27] Innovation, Science, and Economic Development Canada, "Accredited certification bodies," last accessed 21 April 2022, https://ised-isde.canada.ca/site/cybersecure-canada/en/certification-bodies.

73/266, adopted in 2019, called for the establishment of a "Group of Governmental Experts [GGE] on Advancing responsible State behaviour in cyberspace in the context of international security."[28] There are 25 members of this GGE, and although Canada has been active participant during open working groups, is not a permanent member. However, Canada is a co-sponsor for the UN's Programme of Action (PoA) on cybersecurity, with a view to create an action-oriented space where responsible State behaviour is promoted within a framework.[29] As a member of NATO, Canada participates in the NATO Industry Cyber Partnership, which primarily aims to strengthen cyber defences within member countries' defence supply chains.[30] In a 2017 interview, Canadian then-Ambassador to NATO Kerry Buck spoke in favour of multilateral partnerships that would strengthen the defence industrial bases across NATO as a whole.[31]

TO ADOPT OR NOT TO ADOPT?

With two of Canada's principle military allies having adopted programs that certify vendors in their defence supply chains, it would seem intuitive that Canada should simply adopt one of these programs to ensure interoperability and at least bilateral, if not multilateral, industrial and economic benefits. However, the models for both the US and

---

[28] United Nations, Office for Disarmament Affairs, "Group of Governmental Experts," last accessed 21 April 2022, https://www.un.org/disarmament/group-of-governmental-experts/.

[29] Global Affairs Canada, "Canada's submission to UNSC Open Debate on cybersecurity," last accessed 21 April 2022, https://www.international.gc.ca/world-monde/international_relations-relations_internationales/un-onu/statements-declarations/2021-06-29-cybersecurity-cybersecurite.aspx?lang=eng.

[30] North Atlantic Treaty Organization, "Our Objectives and Principles," last accessed 29 April 2022, https://nicp.nato.int/objectives-and-principles/index.html.

[31] North Atlantic Treaty Organization, "NATO, Innovation, and Industry Partnerships: Interview with Canada's Ambassador to NATO," last accessed 28 April 2022, https://www.ncia.nato.int/about-us/newsroom/nato--innovation--and-industry-partnerships-interview-with-canadas-ambassador-to-nato.html.

UK cannot be implemented as-is in Canada, because national accreditation constraints of those nations would prevent Canadian-based accreditors from certifying Canadian companies to provide services or products in those countries. Although allowing foreign accreditors to certify Canadian companies could be a possible solution, there are three main concerns with this option. First, foreign accreditors may not have the Canadian security clearances required for high risk CUI. Second, allowing foreign accreditors to certify Canadian companies for a procurement contract would be against the ISED principles for promoting Canadian SMEs, and would potentially sideline the existing CyberSecure Canada program. Finally, Canada would need to choose between the US and UK programs as adopting both for domestic use would result in conflicting standards between NIST's SP 800-171 publication and ISO 27001.

The importance of bilateral or multilateral arrangements is underscored by the emergence of great power competition in recent years. The rise of Russian and Chinese influence in world politics has highlighted the vulnerabilities in relying on foreign manufacturing for military and defence systems.[32] Strengthening ties within existing alliances, particularly with those closest to Canada in terms of geography and historical importance, will become increasingly important for a middle power like Canada. This paper envisions three possible scenarios for how Canada can address interoperability with allies while protecting Canadian national security and domestic economic interests.

In the first scenario, Canada could broker a new multilateral agreement between participating countries whereby accredited national assessors certify domestic companies

[32] Congressional Research Service, *Renewed Great Power Competition: Implications for Defense—Issues for Congress*, (Washington, D.C.: Congressional Research Service, 2022), 24.

that wish to participate in the coalition's defence industrial complex and handle CUI. This agreement, assuming participation from the US and UK, would require reciprocity clauses and agreement that NIST's SP 800-171 publication is equally acceptable as ISO 27001 and CSE's guidelines. This multilateral agreement would likely implicate CSE in greater engagement with international partners. Further, DND's contract risk assessors would have to consider potential foreign handling of CUI unless PSPC was engaged to limit contracting options to Canadian vendors. Although this scenario would ensure the inclusion of Canadian SMEs and solve some of the problems identified above, the process could be bureaucratic and slow to implement when procurement timelines are already beleaguered with delays.

In a second scenario, Canada would resolve reciprocity limitations with the existing CMCC and CSM programs, such that Canadian assessors of Canadian companies are accepted by DOD and MOD for contracts, and vice versa, according to a mutually agreed upon standard. This scenario could likely be adopted faster than the first, but might require an adjustment of CyberSecure Canada standards. If this reciprocity arrangement could be accepted by the US and UK, then the Standards Council of Canada would need to adjust its accreditation for Canadian assessors who opt to include the US and UK standards. At the same, any currently certified accreditation company in Canada operating under the current CyberSecure Canada programme would still be able to assess companies competing for Canadian contracts.

In the last scenario, which is effectively status quo, Canada continues to use only CyberSecure Canada. Either Canadian companies that handle Canadian CUI are not allowed to compete for US or UK-based contracts where Canadian data might be at risk,

or DND accepts the risk that sensitive information in its defence supply chain is vulnerable to loss of data sovereignty. In this situation, DND could ensure that PSPC enforces the applicable CMMC or CSM certification prerequisite for contracts that include handling CUI. Although not ideal, this scenario would include some level of protection of CUI outside of Canada but with little recourse should the CUI be compromised.

Regardless of scenario, DND must recommend a path for hardening its defence supply chain against cyber security threats. While related to but outside the scope of this paper, in 2021 the Australian Defence Force (ADF) implemented their own Defence Industry Security Program (DISP), which allows Australian companies to register as compliant with one of four possible standards. The DISP allows companies to be compliant with any one of the Australian standard, ASD Essential 8, US NIST standard, the legacy UK defence standard (DEF STAN) 05-168, or ISO 27001.[33]

A 2019 report from the South Australian Defence Industry Leadership Program (SADILP) identified cyber threats to SMEs as a significant vulnerability in the Australian defence supply chain, and identified SME challenges and recommendations to mitigate cyber security threats that are common to Canada.[34] Some measures, such as making online training products publicly and freely available, clearly identifying sub-contractors in bids, and streamlining cyber security advice for contractors handling CUI would be

[33] Australian Industry Group and Department of Defence, *Working Securely with Defence: A Guide to the Defence Industry Security Program membership*, (Canberra: Commonwealth of Australia, 2020), 35.

[34] Jonathan Frank, Molly Davidson, and Neil Morris, "Cyber Security's Impact on SMEs and the Supply Chain," South Australian Defence Industry Leadership Program, November 2019, 7-10. https://dtc.org.au/wp-content/uploads/2020/04/SADILP-2019-Concept-paper-Cyber-Security-Report-FINAL.pdf.

low-cost ways to improve Canada's SMEs' cyber resilience. Other measures such as providing grants to SMEs for implementing cyber protection tools, providing tailored expert advice to SMEs, and imposing fines for data breaches would be either costly or time consuming, but potentially worth further research depending on the course of action chosen for hardening the defence supply chain.[35]

Aside from certifying and regulating individual SMEs or large vendors that handle CUI, an additional approach that would help safeguard DND's data sovereignty would involve investigating Canada's ICT backbone and how data is routed. The concept of network sovereignty involves a Canadian national digital infrastructure strategy, which would seek to improve control over public communications networks.[36] Published in 2019, ISED's "Canada's Digital Charter in Action: A Plan by Canadians, for Canadians" 22-page report speaks to infrastructure, but only as it pertains to improving Internet access within Canada.[37] Whether data residency within one's own national borders results in more secure handling of CUI is a question for debate amongst cyber security professionals. However, transparency by Internet service providers (ISPs) on the sale of data to third-parties and a clear understanding of primary routing paths are measures that have been shown to increase cyber security.[38] The most recent version of the Treasury Board of Canada's Directive on Service and Digital, effective 1 April 2020, does require Canada's Chief Information Officer to ensure that personal, high level CUI, and

---

[35] *Ibid*.

[36] Andrew Clement, "Canadian Network Sovereignty: A Strategy for Twenty-First-Century National Infrastructure Building," last modified 26 March 2018, https://www.cigionline.org/articles/canadian-network-sovereignty/.

[37] Innovation, Science, and Economic Development, *Canada's Digital Charter in Action: A Plan by Canadians, for Canadians*, (Ottawa: Canada Communication Group, 2019), 1-22.

[38] Sean Boots, "Data residency is security theatre," last accessed 29 April 2022, https://sboots.ca/2020/03/29/data-residency-is-security-theatre/.

classified information is stored within Canadian physical boundaries or in a consulate abroad.[39] This type of directive could be similarly implemented within Canada's ICT infrastructure, which would not only benefit Canadians' personal security but also strengthen Canada's defence supply chain through national infrastructure policies.

CONCLUSION

SMEs and larger Canadian companies, even those companies with certified best practices for cyber security, are vulnerable to data loss through targeting and human error. Canadian companies and academic institutions that are known to handle CUI are at risk for targeting with the intent to scrape data, which weakens national security and puts CAF operations at risk. While the private sector has financial incentive to prevent intellectual property loss, the loss of data sovereignty for DND has national security implications. DND, PSPC, CSE, and ISED all play vital roles in minimizing this risk. DND must identify CUI before it is released outside of governmental control and ensure it is released only to companies whose cyber security practices have been certified as compliant with government-approved standards. PSPC must be engaged to ensure that contracting processes enable vendor adherence to cyber security standards. Given the appeal of CUI by adversarial actors, SMEs may be targeted for this information and Canadian SMEs are unlikely to have sophisticated cyber defences. Therefore, CSE must assist in securing the Canadian infrastructure in general and implement active defence measures for registered Canadian vendors in Canada's defence supply chain. Finally, ISED must support SMEs and Canadian economics interests by encouraging bilateral or

[39] Treasury Board Secretariat, "Directive on Services and Digital," last accessed 29 April 2022, https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32601.

multilateral agreements that support transnational reciprocities for cyber security program accreditations.

Canada needs to ensure data sovereignty to protect national interests while ensuring interoperability and multilateral cooperation with allies. The US CMMC and UK CSM programs offer four levels of CUI and MODII classifications, respectively, with increasing levels of compliance requirements as risk increases. However, both programs are limited to domestic assessors and have no provision for Canadian accreditation. The programs differ in their choice of cyber security standard: the US opted for their own NIST SP 800-171, while the UK adopted the international standard ISO 27001. Neither program would be suitable for Canada to adopt as they are currently implemented, but the status quo relies on foreign accreditation of cyber security practices for companies that are part of the Canadian defence supply chain but are not based in Canada. Canada should consider brokering a mutual reciprocity agreement between the US, the UK, and Canada – and perhaps extended to NATO countries – so that the Canadian defence supply chain and those of our allies are collectively stronger and resilient against cyber attacks.

BIBLIOGRAPHY

Australia. Australian Industry Group and Department of Defence. *Working Securely with Defence: A Guide to the Defence Industry Security Program membership.* Canberra: Commonwealth of Australia, 2020.

Blosfield, Elizabeth. "Cyber Lessons for the Insurance Industry Continue Three Years After NotPetya." Last modified 12 August 2020. https://www.insurancejournal.com/news/national/2020/08/12/578788.htm.

Boots, Sean. "Data residency is security theatre." Last accessed 29 April 2022. https://sboots.ca/2020/03/29/data-residency-is-security-theatre/.

Breznitz, Dan. "Data and the Future of Growth: The Need for Strategic Data Policy." Last modified 19 April 2018. https://www.cigionline.org/articles/canadian-network-sovereignty/.

Canada. Canadian Centre for Cyber Security. "Baseline cyber security controls for small and medium organizations." Last accessed 22 April 2022. https://cyber.gc.ca/en/guidance/baseline-cyber-security-controls-small-and-medium-organizations.

Canada. Department of National Defence. *Strong, Secure, Engaged: Canada's Defence Policy*. Ottawa: Canada Communication Group, 2017.

Canada. Department of National Defence. "Supply Chain Risk Management: Initiatives at Department of National Defence, Brief to CIPMM Virtual Summit." 3 June 2021.

Canada. Department of National Defence. Assistant Deputy Minister (Materiel). "Cybersecurity Maturity Model Certification (CMMC) and Canada, ADM Cyber Security Committee," May 2021.

Canada. Global Affairs Canada. "Canada's submission to UNSC Open Debate on cybersecurity." Last accessed 21 April 2022. https://www.international.gc.ca/world-monde/international_relations-relations_internationales/un-onu/statements-declarations/2021-06-29-cybersecurity-cybersecurite.aspx?lang=eng.

Canada. Innovation, Science, and Economic Development Canada. "Accredited certification bodies." Last accessed 21 April 2022. https://ised-isde.canada.ca/site/cybersecure-canada/en/certification-bodies.

Canada. Innovation, Science, and Economic Development. *Canada's Digital Charter in Action: A Plan by Canadians, for Canadians*. Ottawa: Canada Communication Group, 2019.

Canada. Office of the Privacy Commission of Canada. "Frequently asked questions about cookies." Last accessed 19 April 2022. https://www.priv.gc.ca/en/privacy-

topics/technology/online-privacy-tracking-cookies/cookies/frequently-asked-questions-about-cookies/.

Canada. Parliament of Canada. "An Act to amend the Personal Information Protection and Electronic Documents Act and to make a consequential amendment to another Act." Last accessed 3 May 2022. https://www.parl.ca/LegisInfo/en/bill/41-2/S-4.

Canada. Treasury Board of Canada Secretariat. "Directive on Services and Digital." Last accessed 29 April 2022. https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32601.

Canada. Treasury Board of Canada Secretariat. "Government of Canada White Paper: Data Sovereignty and Public Cloud." Last accessed 3 May 2022. https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/gc-white-paper-data-sovereignty-public-cloud.html.

Clement, Andrew. "Canadian Network Sovereignty: A Strategy for Twenty-First-Century National Infrastructure Building." Last modified 26 March 2018. https://www.cigionline.org/articles/canadian-network-sovereignty/.

Eggendorfer, T. "Using third party cookies for forensic identification." *Proceedings of the International Conference on Security and Management (SAM), Athens,* 2015.

Frank, Jonathan, Molly Davidson, and Neil Morris. "Cyber Security's Impact on SMEs and the Supply Chain." South Australian Defence Industry Leadership Program, November 2019. https://dtc.org.au/wp-content/uploads/2020/04/SADILP-2019-Concept-paper-Cyber-Security-Report-FINAL.pdf.

Fruhlinger, Josh. "The CIA triad: Definition, components and examples." Last modified 10 February 2020. https://www.csoonline.com/article/3519908/the-cia-triad-definition-components-and-examples.html.

Google Ads. "Reach new customers online with Google Ads." Last accessed 3 May 2022. https://ads.google.com/home/?utm_source=marketingplatform.google.com&utm_medium=et&utm_campaign=marketingplatform.google.com%2Fabout%2Fresources%2Fanalytics-data-controls-feature-brief%2F.

House, Aleskey. "The Price of a Cybersecurity Culture: How the CMMC Should Secure the Department of Defense's Supply Chain Without Harming Small Businesses and Competition." *Public Contract Law Journal* 50, no. 3 (Spring 2021): 449-470.

IASME Consortium. "Become an Assessor." Last accessed 21 April 2022. https://iasme.co.uk/become-an-

assessor/#:~:text=To%20become%20an%20IASME%20Governance%20Assessor%2C%20you%20will%20first%20need,CISM.

IASME Consortium. “Cyber Essentials; The Benefits of Certification.” Last accessed 21 April 2022. https://iasme.co.uk/cyber-essentials/.

ISO. “ISO/IEC 27001:2013.” Last accessed 21 April 2022. https://www.iso.org/standard/54534.html.

Jarke, Matthais, Boris Otto, and Sudha Ram. “Data Sovereignty and Data Space Ecosystems.” *Business & Information Systems Engineering* 61, no. 5 (Oct 2019): 549-550.

Lisenco, Vladlena. “Improving the practice of Competitive Strategies for the protection of Intellectual Property: the law and economics approach.” *Eastern European Journal of Regional Studies* 7, no. 1 (June 2021): 173-176.

North Atlantic Treaty Organization. “NATO, Innovation, and Industry Partnerships: Interview with Canada's Ambassador to NATO.” Last accessed 28 April 2022. https://www.ncia.nato.int/about-us/newsroom/nato--innovation--and-industry-partnerships-interview-with-canadas-ambassador-to-nato.html.

North Atlantic Treaty Organization. “Our Objectives and Principles.” Last accessed 29 April 2022. https://nicp.nato.int/objectives-and-principles/index.html.

Olsen, John and Martin van Creveld. *The Evolution of Operational Art: From Napoleon to the Present*. Oxford: Oxford University Press, 2011.

Trusov, Michael, Liye Ma and Zainab Jamal. “Crumbs of the Cookie: User Profiling in Customer-Base Analysis and Behavioral Targeting.” *Marketing Science* 35, no.3 (May-June 2016): 405-426.

United Kingdom. Defence Cyber Protection Partnership. *Defence Cyber Protection Partnership Cyber Security Model Industry Buyer and Supplier Guide.* Kew: The National Archives, June 2018.

United Kingdom. Ministry of Defence. “Industry Security Notice Number 2017/01.” Last accessed 29 April 2022. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/594320/DART_ISN_-_V2_3.pdf.

United Nations. Office for Disarmament Affairs. “Group of Governmental Experts.” Last accessed 21 April 2022. https://www.un.org/disarmament/group-of-governmental-experts/.

United States. Acquisition and Sustainment, Office of the Undersecretary of Defense, “About CMMC.” Last accessed 6 April 2022. https://www.acq.osd.mil/cmmc/about-us.html.

United States. Congressional Research Service. *Renewed Great Power Competition: Implications for Defense—Issues for Congress.* Washington, D.C.: Congressional Research Service, 2022.

United States. White House Office of Trade and Manufacturing Policy. *How China's Economic Aggression Threatens the Technologies and Intellectual Property of the United States and the World.* Washington, DC: U.S. Government Printing Office, June 2018.