CANADIAN GLOBAL AFFAIRS INSTITUTE
INSTITUT CANADIEN DES AFFAIRES MONDIALES

Canada's "as is" Contract Security Program and the Aggregate Risk Profile of the Nation

by Ron Lloyd

October 2024

POLICY PERSPECTIVE

CANADA'S "AS IS" CONTRACT SECURITY PROGRAM AND THE AGGREGATE RISK PROFILE OF THE NATION

by Ron Lloyd

October 2024

CANADIAN GLOBAL AFFAIRS INSTITUTE
INSTITUT CANADIEN DES AFFAIRES MONDIALES

Prepared for the Canadian Global Affairs Institute
Suite 2720, 700 – 9th Avenue SW., Calgary, AB T2P 3V4
www.cgai.ca

ISBN: 978-1-77397-317-3

Canada's "as is" Contract Security Program and the Aggregate Risk Profile of the Nation

One of the challenges for large bureaucracies is identifying second and third order effects of risk mitigation postures across the enterprise. In the article *Public Service Culture, Risk Management and Governance: The Prerequisite of Effective Strategic Governance to Realizing Our Digital Ambition*, the concept of an aggregate risk profile was introduced to highlight the potential adverse implications of such postures. The example used in the article was the requirement to amend the classification framework of the nation because in its current construct, it represents an over-mitigation of a lower risk that accrues significant real-world risk. The article also points to the Contract Security Program (CSP) as another example of an "as is" risk mitigation posture that is accruing real-world risk to Canada.

In Canada, there has been a lot of focus put on improving the Contract Security Program to accelerate procurement while concurrently ensuring the security of protected and classified information, assets and access to work sites. The importance of this program is underscored by the *2007 Report of the Auditor General of Canada to the House of Commons*, it's subsequent *Status Report on Security in Contracting* published in the spring of 2013 and the *Evaluation of the Contract Security Program* conducted by Public Services and Procurement Canada's (PSPC) Office of Program Evaluation for the period 2011-2017. Although all three documents observed shortcomings and provided recommendations to improve the CSP, they were all in the context of preserving the status quo policy paradigm. Although they are responsible for the delivery of the CSP, the PSPC must do so within the policy constraints articulated by Treasury Board. As such, implementation of the "tactical" recommendations identified in these reports may alleviate many of the problematic symptoms associated with the CSP. However, absent diagnosing and resolving the strategic problems associated with higher level policies, Canada's aggregate risk will continue to increase.

The aim of this article is to explore in greater detail how the "as is" CSP is providing a false sense of security to government and Canadians. It will also identify a number of second and third order effects that include increasing the overall costs of procurement, the unintended implications for new Canadians looking to supply goods and services to the nation (or work for organizations that do), the corresponding negative impact on realizing diversity and inclusion outcomes and finally, its impediment on the realization of Canada's *Digital Ambition*. The analysis will include examining how some of our closest allies and partners mitigate government procurement risk to ascertain whether there are best practices that Canada should consider. Finally, a number of recommendations to improve the Contract Security Program will be provided to enable Canada to adopt a risk mitigation posture that best meets the requirements of the nation and reduces Canada's aggregate risk profile.

The "as is" Contract Security Program

The policy that articulates the requirement for, and responsibilities to ensure, secure procurement is the *Policy on Government Security* (PGS) (July, 2019). In accordance with the PGS, Deputy

Heads are to ensure that the "Security requirements associated with contracts and other arrangements are identified and documented, and related security controls are implemented and monitored throughout all stages of the contracting or arrangement process to provide reasonable assurance that information, individuals and assets and services associated with the contract or arrangement are adequately protected." For procurements that have a security requirement, of which all digital procurements do, approximately 90 per cent are delivered by PSPC's CSP.

The implications of the CSP on procurement are profound. "Pre-contract negotiations, involving protected or classified information and assets, cannot start before an organization has been security screened through the CSP, unless specified by the contracting authority. This also applies when a security-cleared organization wishes to award a subcontract with security requirements to another organization." There are three types of organization clearances, a provisional security clearance, which is temporary in nature to facilitate bid preparation activities if required, a Designated Organization Screening (DOS), which is required to access Protected A or B information or assets and to obtain a site access status, and a Facility Security Clearance (FSC), which is required to access classified information or assets: Confidential, Secret, or Top Secret and North Atlantic Treaty Organization (NATO), European Union and the European Space Agency equivalents and to obtain a site access clearance.

In the *Standard on Security Screening* (Oct 2014) there are three standard screening criteria: reliability status (valid for 10 years), Secret clearance (valid for 10 years) and Top Secret clearance (valid for five years), in addition to enhanced levels for reliability and Top Secret. The implications of only having three screening criteria result in a minimum requirement of a reliability status for DOS and a minimum requirement of secret clearance for FSC. It is interesting to note that although an individual's status/clearance is valid for five or 10 years the validity of the DOS and FSC are two and one year respectively. When the validity period or a DOS/FSC is up, "if your organization is not participating in another solicitation process or executing a contract or subcontract with security requirements, the CSP will terminate its security clearance".

Another requirement of the CSP is to determine if foreign ownership, control or influence (FOCI) represents a procurement risk. A FOCI evaluation "assesses the degree of authority, ownership, control or influence that foreign interests may have over a Canadian organization. This helps determine and mitigate the risk that unauthorized third parties may exert undue influence over a Canadian organization to access government classified information and assets." The FOCI evaluation consists of answering seven questions related to ownership, foreign personnel in key positions, personnel in key positions that work for foreign entities, contractual agreements with foreign organizations, liabilities to foreign organizations in excess of 10 per cent, and revenue in a fiscal year that exceeded 10 per cent or more from a foreign person, entity or sale.

As Canada has erroneously articulated that the level of injury for the compromise of Secret and Protected B are the same, it is not surprising that the requirements for the DOS and the FSC are very similar. Other than the obvious requirement for different levels of personnel screening, the only difference between the DOS/FSC is all key senior officials need to complete a personnel security screening form for an FSC. The estimated timeline for a DOS is up to four months whereas

an FSC is six months or more. The difference in processing time is largely attributed to being able to conduct reliability screening much quicker than secret screening.

The implications of having very similar procurement security requirements for non-national security and national security procurements are profound. During the last 10 years, the number of companies that have required a DOS/FSC has risen from approximately 12,000 to approximately 27,000 companies. In addition to the many new companies seeking a DOS/FSC each year, the CSP must review approximately 18,000 companies annually, based on the validity periods. To further exacerbate the situation federal crown corporations are also seeking to be included in the CSP despite not being required to do so by policy. Evidence of the tremendous pressure that the CSP is experiencing is the most recent policy update that came into effect in May of 2022.

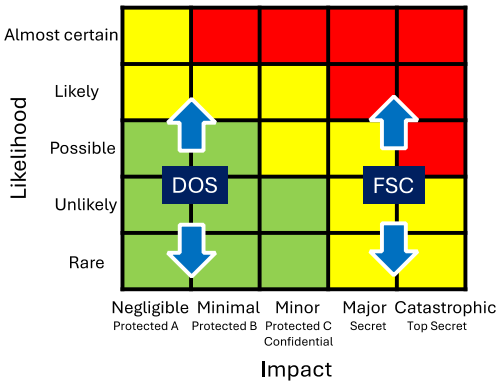
As noted above, a key requirement of the DOS/FSC is ensuring that individuals are issued the appropriate security status/clearance. Although the number of security status/clearances issued to non-public servants has increased significantly to approximately 750,000, the overall representative percentage of clearances has remained relatively constant during the last decade. Approximately two-thirds are reliability, one-third Secret and less than two per cent Top Secret. Essentially there are approximately 490,000 reliability, 245,000 Secret and 15,000 Top Secret clearances issued to non-public servants. Just to sustain the current demand, approximately 75,000 status/security clearances require a renewal each year in addition to those that must be issued to support new procurements before we even take into consideration additional participation by federal crown organizations. The requirement for PSPC to manage the process for the issuing, revoking, and renewing of half a million reliability statuses for low risk procurements is extremely problematic.

As a result, the CSP is currently unable to deliver within the program objectives and DOS/FSC (national security procurement) reviews are currently being risk managed which accrues real world risk.

The CSP in the context of Canada's aggregate risk profile

It is important to underscore that the level of injury for the compromise of protected information is not the same as that of classified information in the national interest of the nation. This fact is supported in the OAG status report of 2013. Even though the policies in effect at the time articulated the same level of risk for each of the corresponding protected and classified classifications, the OAG adapted the framework in Exhibit 2.1 to underscore that Protected Information is less sensitive than classified information. As such, regardless of how you characterize the impact or the likelihood, or how you assign color coding to each of the boxes in the risk matrix, a simple labeling of the security clearances along the bottom of the risk matrix makes it abundantly clear that the FSC and DOS are at opposite ends of the risk management spectrum, as portrayed in Figure 1.

Figure 1: The DOS and FSC are at the opposite ends of the procurement risk matrix.



By definition the impact of a compromised national security procurement will have major or catastrophic impact on the nation. Having to risk manage the FSC to mitigate the negligible to minimal impact of unclassified procurements, with all the attendant negative implications, is increasing the aggregate risk profile of the nation.

Based on the major to catastrophic implications associated with Secret and Top Secret procurements, the rigour of the CSP makes absolute sense as it pertains to the FSC. However, the question that needs to be answered is does the DOS over-mitigate a low risk where the level of investment does not represent value for money, or the opportunity cost adversely impacts the enterprise thereby increasing real world risk? The fact that we are currently risk managing the CSP with potential unintended consequences associated with Secret and Top-Secret contract management would indicate that the answer is yes. In addition, the following second and third order impacts also substantiate that the DOS does not represent value for money and results in significant missed opportunity costs.

As indicated previously, the requirements of the DOS require personnel to be cleared to reliability status. In order for an individual to be issued a reliability status, the following information is required: a five-year background check, verification of identity and background by the individual's Company Security Officer, including education credentials, professional qualifications, and personal and professional references, a credit check and a criminal record check. For Canadians who have lived in Canada for their whole life and have not been out of the country for more than six months in the last five years, or for new citizens who come from a liberal western democracy with which Canada has information exchange agreements, the background check is quite straight forward. However, this is not the case for the majority of new Canadians as a five-year background check can be exceptionally problematic.

The requirement for a permanent resident to become a Canadian citizen is having lived in Canada for three of the last five years. If a new Canadian has lived in Canada for the last three years consecutively and is granted citizenship, however their country of origin is other than a liberal western democracy, their security screening meets one of the three criteria to be characterized as a complex file, the other two being adverse criminality or credit information. A complex file is essentially a screening which requires a background check from a country that Canada does not have an information exchange agreement. Broadly speaking, any country other than a liberal western democracy results in a complex screening. This is extremely problematic because in the Immigration, Refugees and Citizenship Canada's (IRCC) 2023 Annual Report to Parliament on immigration, the top 10 countries from which permanent residents are admitted are India, China,

Afghanistan, Nigeria, Philippines, France, Pakistan, Iran, United States, and Syria. Only two of which have information exchange agreements with Canada (U.S. and France) and they only account for 9 per cent of the top 10 countries. Equally problematic is that the top five emerging source countries Cameroon, Congo DRC, Eritrea, Bangladesh, and Vietnam do not have an information sharing arrangement either.

It is difficult to determine how many reliability clearances are denied because of challenges associated with conducting a background check. As the onus is on government to make every effort to complete the background check, complex files can stay open for years until the CSP validates whether there is still a requirement for the status/clearance. If the requirement is no longer valid then it is closed not denied. However, if the requirement remains it will stay open despite full knowledge that it will not be possible to complete the background check. For new Canadians that are fortunate to be granted a reliability status, the average wait time is months and years not days and weeks. If a reliability status is a pre-requisite to employment, and the wait time is excessive, then it should not be surprising that many of the screenings are not required as new Canadians move on to seek other employment opportunities.

These lengthy wait times for complex files are also well understood by Canadian industry. For companies that provide government goods or services they need to be able to hire employees who are immediately available to work. As such, they can ill afford to hire individuals that will have to wait a considerable time prior to being employable. As all sub-contractors are also subject to the CSP, it can be problematic for SMEs to support a larger prime contractor. For new Canadians who own a small or medium enterprise, they will not be able to compete for government contracts with security requirements or be listed on standing offers until they wait months and years to be granted a status/clearance. As "immigration accounts for almost 100% of Canada's labour force growth, and, by 2032, it's projected to account for 100% of Canada's population growth," based on the current demographics it will be increasingly difficult to employ new Canadians in the federal government or to provide goods and services to government. From a digital perspective, the impact is even more acute.

The annual Digital Update noted that the "GC is in a very competitive situation in attracting the workforce needed to deliver on the Ambition. The GC needs to: represent the population of Canada…" In June 2023 the government released Canada's tech talent strategy. The strategy is based on four key pillars:

1. developing a new Innovation Stream under the International Mobility Program to attract highly talented individuals,
2. promoting Canada as a destination for digital nomads,
3. improving labour mobility in North America,
4. improving existing programs that cater to workers in high-skill tech occupations.

As digital nomads arrive in country keen to work, it will be frustrating for them to have to wait at least two years to be granted a reliability screening. As the reliability status is also a pre-requisite for employment in the Public Sector, the challenges associated with validating a five-year background check are equally problematic. As such, probable challenges associated with attracting and recruiting digital nomads into government may have corresponding adverse implications on diversity and inclusion strategies in government and in the provision of goods and services.

The CSP also has implications with respect to reinforcing legacy digital procurement practices such as staff augmentation or replacement services. As the government is often in a hurry to procure goods and services, often one of the procurement pre-requisites is for individuals or companies to have the appropriate screening completed. Prior to May 2022, this was less of an issue because of the extraordinary pressure that the CSP was under resulting in PSPC to limit screenings to organizations that have a contract or are about to sign a contract. Therefore, companies with existing TBIPs supply arrangements are able to leverage the CSP to provide pre-clearance for individuals. This "backdoor" not only puts additional pressure on the CSP program, but it enables companies to have as many as approximately 20,000 personnel cleared. As a result, there is a steady supply of individuals able to respond to TBIPs procurements, so departments do not have to risk any "security delays". However, for much of the transactional procurement that government requires, it makes it a challenge for new companies to compete because absent a contract or competing on a contract, they can't get into the program. The negative implications from a government perspective are the adverse impacts on small and medium enterprises and outcome-oriented companies who can't compete for procurements that require companies to have clearances "in hand".

Another important implication is that because of overclassification requirements embedded in the security classification framework and the corresponding impact that it has on driving an overclassification culture in government, the DOS undermines sharing information with government. It is not uncommon for information that is securely exchanged between industry partners to be encumbered by the CSP. For example, financial information securely collected by the banks and subsequently exchanged with government is immediately subject to the DOS. In any project in which an industry partner provides an unclassified document to government and someone puts a protected classification on it, the DOS applies. The unintended consequence is that rather than reinforcing security, the application of the DOS in circumstances that are clearly unclassified, undermines the overall security posture and disincentivizes industry to share information with government.

Another element of the CSP that results in increased costs are those associated with multinational procurements. Based on the unique characteristics of Protected B, unclassified information that has the same level of injury as Secret, there is no equivalent amongst our allies or closest partners. Therefore, trying to put in place information sharing agreements is a challenge. For multi-billion, multi-year multinational contracts associated with the significant recapitalization of the Defence sector, the additional requirements of extending the CSP to the non-classified aspects of the procurement represents a significant cost. There are also the inefficiencies that accrue because of

the complexities and challenges of sharing what other allies would characterize as routine information. It also results in tremendous inefficiencies as prime contractors need to onboard subcontractors to the CSP introducing potential implementation risks to the project or program.

There is also a belief that providing a contractor a reliability status mitigates the risk of data compromise. The reality is that "studies have found that most insiders who breach security had no malicious intent when they started their employment. Instead, they may become lax or "go bad" as a reaction to later events". As such, more effective risk mitigation strategies include ensuring information sharing principles such as "need to know" are enforced, cyber security training, and privacy training such as that required by the BC government. It is interesting to observe that federal government contractors are screened to a higher level than most provincial public servants who are also responsible for providing the security and privacy of Canadian citizens information including financial, medical, and other sensitive data.

Finally, another significant consideration with respect to applying the DOS to all contractors is that it adversely impacts leveraging offshore capabilities when it makes sense to do so. For example, provincial governments are leveraging data masking and other digital solutions to leverage offshore expertise and capacity to accelerate and/or cost effectively deliver their digital ambition. Not only are Canadian provinces leveraging this strategy, but so too are many of our Five Eyes partners. Just as Canada leverages a global supply chain, why would it not want to leverage the best of global digital talent particularly when it is realized we don't have sufficient capacity in Canada.

How other nations approach procurement security

It is interesting to note that in the PSPC's Evaluation of the Contract Security Program, conducted by their internal Office of Program Evaluation, that a literature review of similar jurisdictions was completed, and it identifies the U.S. as the only nation that had a similar program. It was also noted that because of the substantial differences in scope, scale, and structure there was limited comparability of the programs. Their conclusion regarding the U.S. is accurate. Since the promulgation of their analysis, if we were to examine how our Five Eyes Partners approach procurement security we would discover that it is clear that they have similar programs and that they prioritize their resources to mitigate higher risk procurements. For example, in Australia, "A security clearance is not required to access information that does not have a security classification, including Official or Official: Sensitive information. For this type of information, routine employment screening is sufficient." Similarly, New Zealand takes a risk management approach for hiring contractors that do not require access to classified information. In the U.K., a third party is responsible for providing a baseline personnel security standard (BPSS). The BPSS is not a security clearance and it provides a three year background check that validates the right to work, identity, criminal check and employment history and confirms no issues associated with out of country travel for periods that exceed six months. Once issued there is no expiry date providing the individual works for the same organization. The BPSS is also required for U.K.

public servants and is used in other sectors such as the financial, energy and communication sectors. In this broad context, Canada is unique in requiring contractors to have a government issued reliability/security clearance for access to non-national security classified information.

With respect to vetting for contractors, once again, Canada has adopted a risk mitigation posture that is out of sync with our Five Eyes Partners and many other nations. The following nations have reported to PSPC whether they require security vetting for access to information or assets classified lower than confidential; the EU, NATO, Five Eyes, Brazil, Chile, Israel, Japan, Singapore, South Africa, South Korea and Switzerland. Of the approximately 44 nations, only ten require vetting of which all of them still recognize the security classification restricted, which Canada does not. The closest of these nations in circumstance to Canada, and that is even a stretch, is Luxembourg. As a frame of reference, Canada has issued more reliability and security clearances to Canadian industry than the entire population of Luxembourg.

Recommendations:

1. The CSP FSC requirements for classified procurements remain as is as they are rigorous and robust.

2. Ideally, the security classification framework of the nation is amended to reflect Official (Official Sensitive), Secret and Top Secret. However, recognizing that this will take time to determine exactly what the security classifications are, it is recommended that the level of injury for Protected A, B, and C be amended to reflect a level of injury lower than the level of injury associated with classified national security information in keeping with our allies and partners and codified in the 2013 OAG Audit Update Exhibit 2.1.

3. In light of the significant adverse implications on the nation's aggregate risk profile, it is recommended that the CSP DOS for non-national security procurements be amended to reflect the Australian model. Specifically, it is recommended that a reliability status is not required to access information that does not have a security classification, including Protected A (Official) or Protected B (Official: Sensitive information). For this type of information, routine employment screening is sufficient. To better mitigate the risk of compromise, prior to granting contractors access to this information, it is recommended that they complete an online training module that ensures they are aware of their responsibilities to protect the information appropriately and the implications if they do not. It is also recommended that the FOCI questionnaire be retained and that it is included as a mandatory document that all departments and agencies ensure is completed by all organizations prior to them providing goods and services to the nation in the event of unanticipated national security implications.

4. Resources that are currently directed to low-risk procurements be re-invested in ensuring high risk national security procurements are no longer risk managed, and additional investment in a more robust FOCI capability.

5. If recommendation #3 is not accepted, amend the DOS validity period to at least seven years, as the screening requirements are good for 10 years and the FSC validity period to five years as that is the validity period of a Top Secret clearance.

6. Personnel screening background checks for a reliability status be amended to three years as opposed to five years in keeping with the U.K. model.

7. Departments that require contractors to access their sites or government IT on an ongoing basis, similar to a public servant, are responsible to ensure contractors are screened to reliability status.

8. A comprehensive stakeholder engagement and robust communications plan be implemented to reinforce the fact that the recommendations better mitigate procurement risk, in addition to addressing unintended second and third order effects.

Conclusion

The Contract Security Program has an exceptionally important role to ensure the security of protected and classified information, assets and access to work sites. Unfortunately, the "as is" CSP is under extraordinary pressure resulting in the overall program to be risk managed. In addition, there are numerous second and third order effects that are equally contributing to increasing the overall aggregate risk of the nation. The real-world risks that continue to accrue include the increased costs of procurement, the impediment to the achievement of the Digital Ambition, the adverse impacts on new Canadians and the corresponding negative implications on diversity and inclusion strategies and finally, reinforcing staff augmentation procurement practices.

Although it is recognized that each nation has its own unique requirements, it is useful to understand how Canada's allies and partners approach procurement security to gain insights on potential best practices. In examining a broad spectrum of nations, and in particular our Five Eyes partners, Canada is over-mitigating non-national security unclassified procurements that do not justify the expenditure of resources at a significant opportunity cost.

In order to adopt a risk mitigation posture that best reflects the needs of the nation to reduce our aggregate risk profile, eight recommendations have been provided. Implementing these recommendations will have tremendous benefits for the nation. The key to their successful implementation will be effective strategic governance based on the depth and breadth of the plethora of policies that will need to be amended to reflect these changes. Adopting a procurement security posture that focuses resources on higher risk procurements and takes into consideration our unique national challenges would be a positive first step to address the false sense of security associated with the current "as is" Contract Security Program.

About the Author

Vice-Admiral (Ret'd) ***Ron Lloyd*** *was the 35th Commander of the Royal Canadian Navy from 2016-2019. During that time he was also "double hatted" as the acting Vice Chief of the Defence Staff for almost half a year and as the first Chief Data Officer for the Department of National Defence and Canadian Armed Forces for a full year.*

During his 38 year career in the RCN, he was privileged to have commanded HMCS CHARLOTTETOWN, HMCS ALGONQUIN, the PACIFIC Fleet and the ATLANTIC fleet. He has extensive operational experience having deployed on numerous occasions globally.

Lloyd has over a decade of experience at National Defence Headquarters having also served as the Deputy Commander of the RCN, the Chief of Force Development for the Canadian Armed Forces, the Director General of Force Development for the RCN and Executive Assistant to the Commander of the RCN.

Today, as Principal of Leadmark Ventures, he shares his experience in leadership, strategic planning and digital transformation with organizations committed to providing innovative solutions that enhance public sector performance in defence and non- defence related activities.

Canadian Global Affairs Institute

The Canadian Global Affairs Institute focuses on the entire range of Canada's international relations in all its forms including trade investment and international capacity building. Successor to the Canadian Defence and Foreign Affairs Institute (CDFAI, which was established in 2001), the Institute works to inform Canadians about the importance of having a respected and influential voice in those parts of the globe where Canada has significant interests due to trade and investment, origins of Canada's population, geographic security (and especially security of North America in conjunction with the United States), social development, or the peace and freedom of allied nations. The Institute aims to demonstrate to Canadians the importance of comprehensive foreign, defence and trade policies which both express our values and represent our interests.

The Institute was created to bridge the gap between what Canadians need to know about Canadian international activities and what they do know. Historically Canadians have tended to look abroad out of a search for markets because Canada depends heavily on foreign trade. In the modern post-Cold War world, however, global security and stability have become the bedrocks of global commerce and the free movement of people, goods and ideas across international boundaries. Canada has striven to open the world since the 1930s and was a driving factor behind the adoption of the main structures which underpin globalization such as the International Monetary Fund, the World Bank, the World Trade Organization and emerging free trade networks connecting dozens of international economies. The Canadian Global Affairs Institute recognizes Canada's contribution to a globalized world and aims to inform Canadians about Canada's role in that process and the connection between globalization and security.

In all its activities the Institute is a charitable, non-partisan, non-advocacy organization that provides a platform for a variety of viewpoints. It is supported financially by the contributions of individuals, foundations, and corporations. Conclusions or opinions expressed in Institute publications and programs are those of the author(s) and do not necessarily reflect the views of Institute staff, fellows, directors, advisors or any individuals or organizations that provide financial support to, or collaborate with, the Institute.