Public Services and Procurement Canada
Services publics et Approvisionnement Canada

Canada

Evaluation of the Canadian Program for Cyber Security Certification: Final Report and Management Action Plan

Cat. No.: P4-176/2026E-PDF

ISBN: 978-0-660-78674-2

Public Services and Procurement Canada

Place du Portage III building 11 Laurier Street, Portage III, Gatineau Quebec K1A 0S5

Aussi disponible en français

Contents

Introduction

The Canadian Program for Cyber Security Certification (CPCSC) is a Government of Canada (GC) initiative directed towards enhancing cyber security for suppliers involved in federal defence contracts. The GC's supply chains are subject to frequent, sophisticated and malicious cyber activity with threat actors increasingly targeting large organizations indirectly through vulnerabilities within their broader supply chain. In response to the current context, the Government of Canada created the CPCSC to strengthen Canadian defence supply chain protections and help safeguard the GC's contractual information.

Defence procurement in the GC is undertaken by PSPC as mandated by the *Department of Public Works and Government Services Act* that requires PSPC to provide acquisition services to federal departments and agencies. Under this mandate, PSPC handles the procurement of goods and services for the GC and offers administrative support and tools to federal organizations, aiding them in delivering programs and services to Canadians.

Overview of the CPCSC

In the fall of 2023, TB approved the CPCSC with the intent to establish mandatory cyber security requirements for suppliers that bid or work on GC defence contracts.

The goals (outcomes) of the CPCSC are as follows:

- Protect federal contractual information held below the classified level on contractors' systems, networks and applications;
- Maintain Canadian industry's access to international procurement opportunities with similar cyber security certification requirements;
- Boost the basic level of cyber security for Canada's defence industry;
- Ensure that the supplier system stays strong and reliable for Canadian Armed Forces capabilities and readiness; and
- Increase Canadian industrial participation in the cyber security certification program.

The CPCSC is led by PSPC's Defence and Marine Procurement Branch (DMPB), specifically the CPCSC Secretariat, which has the responsibility for initiative design and implementation. DMPB is supported by Departmental Oversight Branch (DOB) as the Technical Authority and business owner in support of DMPB project delivery while also leading the development of future design requirements. Procurement Branch (PB) supports the data repository system. Further inputs and supports are provided by a multi-departmental team including Department of National Defence (DND) as the client, Standards Council of Canada (SCC) as the accreditation body, the Communications Security Establishment's (CSE) Canadian Centre for Cyber security (CCCS) as the cyber security technical experts, and Treasury Board Secretariat (TBS) providing policy guidance and updates. Oversight is provided by the Director General-Cyber Security Certification Steering Committee. Budget 2023 identified $25 million (including $13 million in new funding) for the design and implementation of the CPCSC over the period of 2023-2024 through 2025-2026.

CPCSC levels of certification

Once fully implemented, suppliers seeking to bid or work on select GC defence contracts may require certification under CPCSC. The required levels of certification for defence suppliers will be determined on a contract-by-contract basis and will be clearly articulated in Requests for Proposals (RFPs) and contract clauses. The initiative's cyber security certification requirements will be made up of three levels:

- Level 1: requiring an annual cyber security self-assessment;
- Level 2: requiring an triannual external cyber security assessment led by a Certified Third-Party Assessor Organization and an annual affirmation of compliance; and
- Level 3: requiring a triannual cyber security assessment conducted by the Department of National Defence and an annual affirmation of compliance.

The creation of the CPCSC followed the announcement of the creation of the Cybersecurity Maturity Model Certification (CMMC) program in the United States (US), which aims to protect US federal contract information and US controlled unclassified information (CUI) shared with Department of Defense (DoD) contractors. CPCSC is intended to bolster data safeguarding shared with Canada's DND contractors and subcontractors, by applying a Canadian version of cyber controls defined in the Canadian Centre for Cyber Security's (CCCS) Information Technology Security Publication (ITSP) 10.171 / 172 guidance.

CPCSC design and implementation activities

Activities to support the design of the CPCSC were undertaken during the fiscal years of 2023-2024 and 2024-2025. A "soft launch" of the CPCSC was initiated in March 2025, the first of a four phase implementation process. The key purposes of the Implementation Phase 1 (soft launch) are to:

• test the functional use of a repository for contractor data including certifications as well as the self-assessment tool to be used by Contractors;

• test functionality requirements of DND and PSPC procurement officials that need to validate certification completion prior to contract award;

• develop the capacity and knowledge of CPCSC with stakeholders including Canadian companies;

• release the Canadian Industrial Cyber Security Standard based on the US National Institute of Standards and Technology[1] (NIST) standard.

CPCSC implementation plans aim to execute the three additional phases from fall 2025 through 2027[2]. During this implementation, all three levels of cyber security certification are to be introduced into applicable defence contracts.

[1] This is a U.S. government agency within the Department of Commerce. Its mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology.
[2] *The CPCSC received three years of funding its design and implementation activities (for the period of 2023-2024 through to 2025-2026). Planned activities beyond this timeframe were unfunded at the time of this evaluation.*

About this evaluation

The evaluation of CPCSC was conducted by PSPC Evaluation Services Directorate (ESD) between April and June 2025 under the authority of the Head of Evaluation for PSPC.

This mandatory evaluation was included in PSPC's Departmental Evaluation Plan for the period of 2024-25 through 2026-2030.

PSPC's management action plan in response to the findings of this evaluation is presented in Annex 1: Management Action Plan of this report.

Evaluation objective

The purpose of the evaluation was to undertake a formative assessment of the CPCSC so as to support decision-making regarding the future of the initiative. The evaluation assesses PSPC's activities in support the CPCSC with input from the other GC departments and agencies that supported its implementation activities.

Evaluation approach

The evaluation undertook targeted examinations of relevance, effectiveness, and delivery.

Relevance: the evaluation undertook a review of domestic and international programing; examined the importance of recognition of Canadian certification by the US, and studied possible alternative mechanisms that could be considered for achieving CPCSC's intended goals.

Effectiveness: the evaluation focused on understanding the extent to which CPCSC key design, planning and implementation activities have been undertaken as planned to date.

Delivery: the evaluation focused on assessing stakeholder engagement and its contribution to CPCSC implementation, the extent to which risk management practices have been employed, as well as the prioritization of activities and available resources.

The evaluation was conducted using the following lines of evidence:

- **document review**: program planning documentation, governance documents including committee meeting minutes, cyber security research material, budgeting information and industry stakeholder engagement documents were reviewed;
- **interviews**: interviews were conducted with 9 CPCSC stakeholders from PSPC program management (DOB and DMPB), PSPC working level (DOB and DMPB), and TBS (program management); and
- **surveys**: two separate surveys were administered to CPCSC stakeholders from both the working level and program management from PSPC, DND, SCC, TBS, CSE-CCCS, Canadian Commercial Corporation (CCC), and Public Safety.

Limitations stemming from the data collection methods were mitigated to the extent possible by the fact that the findings are from multiple lines of evidence. A discussion of the specific

limitations that impacted the evaluation and the mitigation measures taken to address them can be found in Annex 2: Evaluation Methodology.

Evaluation scope

The evaluation examined CPCSC activities between the period of April 2023 through June 2025. The evaluation reviewed the activities and results of the Engagement, Implementation Preparation and Implementation Phase 1 steps of the CPCSC. So as to ensure that a final evaluation report would be available to support decision making on the future direction of the CPCSC, the final 9 months of operation by the CPCPC under its initial funding have not been covered by this project.

Key findings

The findings from this evaluation are presented under the issues of Relevance, Effectiveness, and Delivery.

Issue 1: Relevance

Summary

The evaluation found the CPCSC to be relevant to on-going GC needs in its purpose to safe guard the accessing, transmitting, and storing of federal non-classified, but deemed sensitive, contractual information.

The evaluation noted that other countries also have national cyber security programs with similar goals to the Canadian program, including the US Cyber Maturity Model Certification program. The review of international programs provided examples of mechanisms for strengthening support for initial entry into the certification programme.

With regards to the US program, the evaluation found that while reciprocity between it and the CPCSC could potentially bring efficiencies to the Canadian program as well as benefits to industry, there continues to be a need for the CPCSC to support its other and equal goals of protecting federal sensitive information; strengthening Canadian defence industry cyber security; and maintaining the integrity of the Canadian Armed Forces CAF supply system.

When ask about potential alternative mechanisms to achieve the goals set for the CPCSC, the integration of the CPCSC into other existing PSPC programs such as the Contract Security Program and Controlled Goods Program was the most frequently suggested possibility.

1.1 Domestic and international program comparison

1.1a Government of Canada programs

The GC has a number of security and procurement programs, in addition to several programs that aim to strengthen cyber security of Canadian businesses and contractors. The evaluation conducted an analysis of current federal programs related to procurement and cyber security to assess for potential duplication of services with CPCSC. The evaluation found similarities among programs but found no evidence of duplicated services by the CPCSC. The CPCSC was found to be unique in its specific focus on enhancing cyber security for defence suppliers, which is distinct from other programs aimed at broader economic development, innovation, or specific sectors.

The evaluation found that Cyber Secure Canada (CSC) (Innovation, Science and Economic Development Canada) displayed the closest similarity with CPCSC. While CSC catered to small and medium-size enterprises (SMEs) across all sectors of the Canadian economy, both programs aimed to enhance cyber security among Canadian businesses by providing certification, training, and guidance. While CSC was discontinued as of March 31, 2023, the authority held by it to accredit organizations to certify SMEs was transferred to SSC. This discontinuation underscores the critical role of CPCSC in maintaining and raising the cyber security baseline within Canadian industry. CSC was referenced by several interviewees as providing important lessons learned for the development of the CPCSC including that a voluntary approach to cyber security assessments was not effective.

The analysis also noted similarities between the CPCSC and two PSPC led programs, the Contract Security Program (CSP) and Controlled Goods Program (CGP), which are managed by the Departmental Oversight Branch. The evaluation found that these programs currently complement each other and the CPCSC and that there is no duplication of services.

The similarities to CPCSC by the CSP and CGP pertain to assurances and safeguarding domain compliance. For example, both the CGP and CPCSC require organizations to implement security measures to safeguard controlled goods and technical data as defined under the Controlled Goods regulation as well as related information as part of government contracting processes while also conducting compliance inspections and security assessments. The CSP and CPCSC also share common objectives and safeguarding assurances based on compliance measures and a series of controls applied to organisation clearances and to contractor employees via personnel screening. Both also support the development of security clauses in contracts and provide training, guidance, and tools to enhance information security. Lastly, all three programs require constant engagement and liaising with the same target consumer of the programs: Industry. Each program requires front line support, outreach and training. These programs also serve to streamline the industry intake process to obtain confirmation of pre-contractual security requirement compliance. However, these programs are distinctively managed. The CSP is managed under the security authorities of the Policy on Government Security and is not mandatory to GC Client organisations. Meanwhile, the CGP is governed by the Defence Production Act and Controlled Goods Regulations and is mandatory for all Canadian entities (except federal organisations) intending to possess and or access controlled goods as defined under the Regulations. In contrast, the soft launch of the CPCSC would be managed under the Policy on Government Security and defined under the Canadian Security Establishment (CSE) promulgated the ITSP 10.171 and ITSP 10.172 standards where the main focus remains the protection of non-classified yet deemed sensitive information in GC contracts.

1.1b International programs

Due to the increasing frequency and sophistication of cyber threats, nations are rapidly enhancing their domestic cyber security measures. To assess alignment of the CPCSC with other national cyber security programs and to identify potential best practices, the evaluation reviewed the programs of its 'Five Eyes' intelligence alliance. The programs assessed included:

- US Cyber Maturity Model Certification (CMMC)
- UK Cyber Security Model (CSM)
- Australia's Defense Industry Security Program (AU DISP)
- New Zealand's Defense Industry Security Program (NZ DISP).

The evaluation found all 4 programs shared a similar primary goal of protecting federal information accessed through contracting, with the New Zealand and Australia programs also focusing on the defence industry. In addition, the goals of the 4 programs included increasing the cyber security baseline of their national industries as well as maintaining supply system integrity. Unlike Canada, maintaining industry access in external procurement markets is not an explicit goal of the 4 programs reviewed.

The evaluation also found that cost to industry is a major concern for all cyber security programs reviewed. In the case of Canada, CPCSC Secretariat-led industry engagements in May 2024, reported 46% of sub-contractors expecting to invest less than$50,000, while 29% of consultants projected costs of $150,000-175,000. 68% of respondents want comprehensive support: financial assistance, guidance, and resources in order to prepare for CPCSC assessment. The evaluation found that each international program also has associated costs for certification, implementation, and maintenance, which can be significant, especially for SMEs. Both Australia and UK seek to support their cyber security industries through their programs, by providing loans and regional development funds (Australia), and mitigating costs through self-assessments and minimum control requirements (UK).

1.2 Reciprocity with United States program

The CPCSC intends to maintain Canadian industry’s access to international procurement opportunities with similar cyber security certification requirements, including the US’s CMMC. Currently, the CMMC Final Program rule would not allow bilateral reciprocity certification programs between another country and the US Department of Defense. DOB’s Industrial Security Division continues their negotiations with the US’s Defense Technology Security Administration (DTSA) to update their existing Canada-US bilateral industrial security MOU.

The evaluation examined the importance of maintaining Canadian industry’s access to international procurement opportunities with similar cyber security certification requirements. Evaluation respondents (interview and survey) noted that the lack of a reciprocity agreement is a potential risk to the program's relevance and value. Several respondents remarked that the greatest impact would be reduced interest and satisfaction with the CPCSC by industry, due to the potential duplication of costs and efforts for contractors needing both CPCSC and CMMC certifications. Both interview and survey respondents also noted that this burden would particularly affect small and medium enterprises (SMEs) as they typically have less resources to allocate to these additional costs. Multiple working level interviewees suggested that the CPCSC

should consider increasing industry engagement activities to boost awareness and buy-in for the CPCSC, especially considering recent developments regarding the lack of a reciprocity agreement. Interviewees also highlighted that lower demand from industry could decrease the need for certified third-party assessor organizations and SCC's accreditation services, potentially harming SCC's cost recovery model, which depends on consistent demand for its services.

A document review of industry consultations conducted by CPCSC Secretariat (prior to the US decision to prohibit bilateral reciprocity agreements with other countries), supported these survey and interview responses. A majority of industry contractors expressed a strong preference for the CPCSC if it were fully reciprocal with US CMMC. Respondents expected a CPCSC backed by a reciprocity agreement with the US to significantly impact their ability to win US defence contracts and be considered compliant to access US defence markets and supply chains.

Although survey and interview respondents recognized the potential impacts of not having a cyber certification reciprocity agreement on the CPCSC's value and relevance, they generally agreed that the initiative remains relevant. The majority of program management interviewees noted the CPCSC continues to address the need to protect sensitive contract information, improve cyber security hygiene by industry and fulfil the need for a domestic program. A review of relevant policy documents confirmed that the CPCSC aligns with the GC's cyber security approaches as set out in the GC Enterprise Cyber Security Strategy (2024), the National Cyber Security Strategy (2022) and Bill C-8, which collectively aim at strengthening Canada's cyber resilience.

Several interviewees at operational and program management levels supported the idea of potentially seeking to establish cyber certification reciprocity with other national cyber security programs—such as the other "Five Eyes" partners (U.K., Australia, New Zealand) and European Union (EU) while another expressed concern that significant differences between these programs could create major obstacles to achieving certification reciprocity.

1.3 Alternative mechanisms

The CPCSC introduced a multi-departmental partnership to initiate the introduction of cyber security protocols for suppliers and their integration into contracting requirements, while also initializing an innovative approach to cross-branch delivery within PSPC. The current CPCSC management model, as currently administered by DMPB, was designed to be temporary with a reassessment and transfer of management to another entity following program implementation. The evaluation conducted an analysis of alternative mechanisms or processes that could be considered for achieving three of the five CPCSC's goals.(protecting federal information; strengthening Canadian defence industry cyber security; and maintaining the integrity of the CAF supply system).

CPCSC stakeholders were consulted during CPCSC implementation on whether they were aware of any potential alternative mechanisms to achieving its outcomes. While the possibility of integrating the CPCSC under the recently announced defence procurement agency was noted by some interviewees, several interviewees at both the operational and program management levels suggested that the CPCSC (currently administered by PSPC's DMPB) could potentially be well integrated with other existing PSPC-led contracting programs focused on information

security, —specifically, the Contract Security Program (CSP) or the Controlled Goods Program (CGP) located in PSPC's DOB. It was noted that the CSP is a policy-based program and thus more flexible, which would allow for easier integration, compared to the CGP which is governed by legislation, making it harder for integration. Respondents cautioned that these other programs are not currently and distinctively tracking how the current compliance assurance measures align with the ITSP10.171 cyber security controls and noted that significant alignment and restructuring could be required to integrate the CPCSC into either program. Respondents noted that restructuring could need to include steps to increase cyber assessment knowledge and expertise to better implement and integrate additional cyber controls in existing security program business lines when transitioning the CPCSC to a new owner.

Multiple program management interview respondents indicated that cyber security requirements could be legislated or regulated for all defence contracts. This could eliminate the need for a certification program and instead involve establishing rules and ensuring compliance through government auditing and oversight. Meanwhile, program management survey respondents were divided on whether alternative mechanisms could achieve the CPCSC's goals, with respondents reporting that no alternative mechanisms were being actively considered at the time the question was posed to them.

The evaluation's assessment of international programs also identified potential alternative mechanisms that Canada could consider adopting to improve the efficiency and effectiveness of the program. This includes a model (UK) for non-compliant suppliers in which suppliers who fail to attain CPCSC certification are required to complete a cyber implementation plan, which outlines the steps they will take to achieve compliance with the cyber security standards. This model also includes a basic entry-level tier (Level 0 tier) of CPCSC Level 1 certification with the only very basic, necessary controls representing very low level of assessed cyber risk, to better the process to attain Level 1. Several interviewees suggested that CPCSC could explore providing financial and technical support to CPCSC participants, similar to the supports offered to participants of the UK and Australia's national cyber security programs. The evaluation noted the Australian program included loans and regional development funding and that the UK program aimed to mitigating costs through self-assessments and minimum control requirements.

Issue 2: Effectiveness

Summary

The CPCSC has encountered slower implementation than originally anticipated due to factors such as the need to redevelop it with a Canada-only focus in early 2025. Key milestones achieved to date include external stakeholder engagement and awareness activities as well as the release of the Canadian Industrial Cyber Security Standard.

2.1 Implementation Status

The CPCSC received its funding and authority to proceed with initial program implementation in March 2023. The evaluation undertook a review of the extent to which key CPCSC activities have been undertaken to date and what have been the results to date from the initiative.

Preparations for the CPCSC's soft-launch began in the summer of 2024. Activities included industry engagement such as webinars to present details of the CPCSC and supplier requirements and a Request for Information issued to Canadian industry including defence contractors, sub contractors, cyber security/IT consultants and IT service providers.

CPCSC's soft launch, originally planned to run from January to June 2025, was delayed until March 2025 (with current estimation of completion in December 2025). This delay was due to the impact of having been unable to establish a pathway to reciprocity with the US program upon initialization of the CPCSC. The CPCSC required time for deliberations on pivoting to a Canada-only model and to undertake a re-design prior to its launch.

To date, while some key deliverables have been achieved, many other implementation milestones have been delayed to fall 2025 and winter 2026, including foundational deliverables such as the application of CPCSC level 1 (Self-Assessment) requirements on pilot contracts, which would act as important test cases for the new CPCSC requirements.

Amongst soft launch deliverables which have been completed, working level and program management CPCSC survey and interview respondents concurred with key achievements to date: identifying the release of the Canadian Industrial Cyber Security Standard, and internal/external stakeholder engagement and awareness activities, including supplier engagement and industry presentations.

Table 1: CPCSC deliverable completion status[3]

Completed on time	Completed late	Due – Delayed	Not yet due
5 of 26 (19%)	2 of 26 (8%)	9 of 26 (35%)	10 of 26 (38%)

Interviewees at both the working and program management level generally noted that CPCSC implementation has been slower than originally anticipated, with respondents noting delays to be the result of the unexpected inability to reach a reciprocity agreement with the US as well as impacts from ongoing Canada-US bilateral industrial security negotiations to update the existing Canada US MOU equivalencies. Interviewees remarked that delays were primarily due to the interdependence of the initiative's activities, with soft launch deliverables having been postponed in some cases because prerequisite and related deliverables were not yet completed. Interviewees also noted the complexities associated with the horizontal nature of CPCSC's implementation involving various government departments, and while also expressing their perceptions of insufficient capacity or accountability in terms of personnel, expertise, and resources within CPCSC. The evaluation's document review noted that most delayed CPCSC soft launch activities are at least partly attributable to an interdependency with one or more implementation activities, supporting a rationale provided by respondents.

[3] *The evaluation is tracking a total of 26 deliverables. 16/26 were due by or before June 2025, and 10/26 are not yet due*

Issue 3: Delivery

Summary

A formal governance structure has been established for the CPCSC with evaluation respondents reporting overall satisfaction with the secretarial support provided by PSPC while also identifying a need to further clarify roles and responsibilities in the administration of the CPCSC.

The evaluation notes that certain key project management tools have yet to be finalized and that there are opportunities to strengthen risk management products in particular.

Stakeholders emphasized the importance of reviewing resource prioritization noting operational areas which did not receive direct funding as part of the CPCSC's authorities.

3.1 Roles and Responsibilities

Stakeholder relationships and coordination play a key role in CPCSC, as 5 different GC departments are responsible for contributing to its implementation. The evaluation undertook an assessment of stakeholder (internal to PSPC and external to PSPC) contributions to the effective implementation of the CPCSC.

A document review was conducted on management materials to better understand the identification of roles and responsibilities. The evaluation found that the CPCSC is supported by a clearly defined governance structure comprised of cyber security committees. This includes a committee at the Assistant Deputy Minister (ADM) level which oversees GC cyber security policies and operations more broadly, as well as committees at the Director General (DG), and Tiger Team working level, which are directly responsible for the implementation of CPCSC. It is further enabled by Defence Procurement Strategy committees at the DM and ADM levels. Committees were found to provide a platform to provide briefings and receive senior level oversight and decision-making regarding CPCSC direction.

Roles and responsibilities of CPCSC contributors were found to be defined across several documents such as a Charter[4] and a Management Framework, however, these documents are still in development and are yet to be approved. The evaluation noted areas where clarity in roles and responsibilities could be enhanced in these documents, such as: transition activities and timeline activities; knowledge transfer activities; communications and risk management.

The Tiger Team Working Group was established in 2022-2023 to support a Cabinet request and has continued to support the CPCSC with long standing members. A survey of Tiger Team members found that members had a clear understanding of the purpose of their working group as well as their individual roles and responsibilities. Respondents also indicated their individual

[4] *While the CPCSC is not a formal project subject to the Treasury Board Directive on the Management of Projects and Programmes, the CPCSC did implement key management tools to support its initial implementation, such as those referenced in this report.*

roles and responsibilities on the working group were appropriate. Overall, Tiger Team Working Group Members from other departments reported satisfaction with the secretarial support provided by PSPC while also expressing a need to further clarify roles and responsibilities of the various organizations to better support activities at the working level and the initiative overall. Additionally, the majority of operational interviewees noted that the CPCSC could raise its efficiency and effectiveness by improving its communication and engagement activities among its organizational stakeholders. Interviewees further indicated that initiative tools could be better maintained and shared amongst stakeholders by the CPCSC Secretariat.

There was a consensus among operational and program management interviewees that CPCSC roles and responsibilities are generally clear, with some describing clarity as improving over time. Interviewees expressed the perspective that the effectiveness of the CPCSC delivery could be further strengthened by better clarification of roles and responsibilities amongst the GC stakeholder departments supporting its implementation. The evaluation document review noted that some actions have been taken to date in this area, with DOB having led two tabletop exercises in April and July 2025 with stakeholder departments with the aim of further defining roles and responsibilities across the various CPCSC related activities.

Internal to PSPC, DMPB currently oversees the design and delivery of the CPCSC for the duration of the soft launch. The temporary model introduced to initialize delivery of the CPCSC is innovative and has required that DMPB and DOB work closely on implementation activities. With regards to the execution of the approach, the evaluation found that the majority of working-level interviewees noted DMPB, whose role is defence procurement and policy development and implementation, had limited cyber security expertise at the time the CPCSC was initiated and raised concerns that this likely hindered DMPB's ability to support its implementation activities. Program management interviewees emphasized the need to clearly define roles and responsibilities before deciding on the future of the CPCSC, including the possibility of management transfer. Program management also underscored the importance of a well-planned transition when management of the CPCSC is moved from DMPB to another organization.

Working and program management interviews indicated that while stakeholder roles are generally appropriate, there is insufficient personnel and technical cyber security expertise within CPCSC stakeholder departments, which may be limiting implementation results to date. A lack of cyber security expertise was reported to extend GC wide. Several interviewees recognized the CSE-CCCS as the primary source of cyber security technical expertise for CPCSC and noted their limited involvement to date, citing a lack of funding and capacity as a barrier. The evaluation noted the absence of a clearly defined role in foundational documents regarding the participation by the CSE-CCCS.

There is a potential risk that if current roles and responsibilities are not updated to take into consideration identified gaps, strengthen stakeholder accountability and prepare for any possible re-location, CPCSC implementation may be further delayed, affecting the timely and effective achievement of its deliverables.

Recommendation 1: It is recommended that PSPC clarify stakeholder roles and responsibilities in program documentation to better enable the effectiveness and efficiency of the CPCSC in both the short-term (while under management by DMBP) and the long-term (once decisions regarding management for the CPCSC are made).

3.2 Risk Management

Understanding and mitigating risks are essential to the achievement of results. The evaluation conducted a review of the CPCSC risk management tools and engaged with stakeholders on the extent to which risk management practices have been effectively implemented.

A document review found that risk management information is detailed across several distinct CPCSC products, such as the Management Plan, Risk Register, and Charter, with further references in authority documents. Many of these documents were still under development and not yet finalized, with the CPCSC Secretariat acknowledging that further work was to be done. The document review included a review of a DOB compiled list of gaps, which was shared with all CPCSC members for review and feedback. The intent of the list was to identify and track gaps within CPCSC's risk management practices in order to better perform mitigation activities. The evaluation noted opportunities for strengthening understanding and mitigation of risks across documents. This included improving completeness, as many risk statements often lacked details on risk event drivers as well as the potential impact should they materialize. It also included enhancing the assessments of likelihood and impact (either quantitative or qualitative) as well as the rating or prioritization of risks as these were often unavailable. The review noted a lack of systematic coverage, finding no evidence of the use of a risk taxonomy to support a comprehensive identification of risks. Furthermore, it was noted that broader, strategic risks to longer-term success of the initiative were considered in lieu of assessment of risks to its initial implementation. The document review noted that roles and responsibilities related to risk monitoring were identified, however, the responsible party for the activity was not included. Finally, the document review noted risk management activities yet to be completed, such as: risk monitoring and control activities; contingency and response plans; and risk reporting.

The majority of survey responses (working level and program management) indicated that while conversations regarding risk had taken place at least to some extent, when asked whether risk management tools had been used to help inform planning and CPCSC implementation, respondents were split on their awareness on the extent to which risk management had been integrated into their work. The majority of respondents also indicated there were past, current or emerging risks, which may not be fully addressed. The following list includes risks indicated as those not fully addressed by working and program management level survey respondents and interviewees at the time the question was posed to them:

- SMEs struggling with the financial and technical demands of implementing and auditing CPCSC standards;
- changing geopolitical landscape and the issues to establishing reciprocity;
- insufficient personnel, project management and technical cyber security expertise within CPCSC stakeholder departments;
- inconsistent stakeholder priorities, coordination, and engagement (noted by Program Management, not by operational interviewees);
- lack of CPCSC testing, as DND has not yet identified a contract;
- unclear plans to transfer CPCSC management following initiative implementation.

There is a potential risk that as CPCSC risks mature, new issues will continue to emerge, which require that the CPCSC have in place a systematic and rigorous approach for tracking, monitoring and reporting of risks and mitigation strategies and how CPCSC is addressing them.

Recommendation 2: It is recommended that PSPC review, strengthen and finalize the risk management tools used by the CPCSC.

3.3 Resource prioritization

Resource prioritization is an important component of project management as it allows for the focusing of limited resources on the most important tasks. The evaluation examined how CPCSC activities are prioritized given available resources and initiative complexity.

PSPC spending on CPCSC has seen 85% of planned budget expended in the first two fiscal years of its operation (2023-2024 and 2024-2025). DMPB spent 70% of its planned budget for fiscal year 2023-2024 and 84% for 2024-2025. DOB spent 0% of its planned budget in fiscal year 2023/24 (as DOB activities had not yet started) and spent 97% of its planned budget in fiscal year 2024-2025.

Working-level interview and survey respondents identified resource allocation and prioritization as a key factor affecting stakeholder coordination and initiative implementation, noting an imbalance where some stakeholders received funding while others did not. The evaluation noted PSPC and SCC as the stakeholder departments receiving funding to aid in the implementation of the CPCSC. Though DND, TBS, and CSE-CCCS are responsible for several implementation activities, they were not provided funding. Both working level interview and survey respondents indicated CSE-CCCS specifically as a stakeholder for which a lack of resources may be impacting their ability to contribute to CPCSC implementation. Multiple interviewees at both the working level and program management level also expressed the possible need to rebalance resources.

CPCSC stakeholders at both working and program management levels from various departments shared various ideas of what should be prioritized as the CPCSC's implementation is finalized. These included increasing testing of CPCSC components to identify and address gaps and increasing use of project management exercises such as RACI to further clarify stakeholder roles and responsibilities. In addition, it was suggested that industry engagement should be increased to boost CPCSC awareness and buy-in, however interviews noted that CPCSC was not provided funds for industry engagement or program promotion.

Evaluation Summary

The Canadian Program for Cyber Security Certification (CPCSC) is a Government of Canada (GC) initiative directed towards enhancing cyber security for suppliers involved in federal defence contracts. The CPCSC is administered by PSPC with support from the following external stakeholders: Department of National Defence (DND) (as the client), Standards Council of Canada (SCC), the Communications Security Establishment's (CSE) Canadian Centre for Cyber

security (CCCS), and Treasury Board Secretariat (TBS). Budget 2023 identified $25 million (including $13 million in new funding) for the CPCSC for the period of 2023-2024 through 2025-2026. At the time of this evaluation, the CPCSC was implementing its 'soft launch' with the intent to establish its foundational elements. To date, no potential contracts have been identified for the piloting of the CPCSC.

The evaluation undertook targeted examinations of relevance, effectiveness, and delivery covering the period of April 2023 through June 2025.

The evaluation found the CPCSC to be relevant to on-going GC needs in its purpose to safe guard the accessing, transmitting, and storing of federal non-classified but deemed sensitive contractual information.

The evaluation noted that other countries also have national cyber security programs with similar objectives to the Canadian program, including the US Cyber Maturity Model Certification program. The review of international programs provided examples of mechanisms for strengthening support for initial entry into the certification programme.

With regards to the US program, the evaluation found that while reciprocity between it and the CPCSC could potentially bring efficiencies to the Canadian program as well as benefits to industry, there continues to be a need for the CPCSC to support its other and equal goals of protecting federal sensitive information; strengthening Canadian defence industry cyber security; and maintaining the integrity of the CAF supply system.

When asked about potential alternative mechanisms to achieve the goals set for the CPCSC, the integration of the CPCSC into other existing PSPC programs such as the Contract Security Program and Controlled Goods Program was the most frequently suggested possibility.

A formal governance structure has been established for the CPCSC with evaluation respondents reporting overall satisfaction with the secretarial support provided by PSPC while also identifying a need to further clarify roles and responsibilities in the administration of the CPCSC.

The evaluation notes that certain key project management tools have yet to be finalized and that there are opportunities to strengthen risk management products in particular.

Stakeholders emphasized the importance of reviewing resource prioritization noting operational areas which did not receive direct funding as part of the CPCSC's authorities.

The evaluation has made the following recommendations:

Recommendation 1: It is recommended that PSPC clarify stakeholder roles and responsibilities in program documentation so as to better enable the effectiveness and efficiency of the CPCSC in both the short-term (while under management by DMBP) and the long-term (once decisions regarding the final location for the CPCSC are made).

Recommendation 2: It is recommended that PSPC review, strengthen and finalize the risk management tools used by the CPCSC.

Annex 1: Management Action Plan

Recommendations	Management Response	Management Action Plan	Deliverables	Targeted Implementation Date	Responsible
1. It is recommended that PSPC clarify stakeholder roles and responsibilities in program documentation so as to better enable the effectiveness and efficiency of the CPSPC in both the short-term (while under management by DMBP) and the long-term (once decisions regarding the final location for the CPCSC are made).	Agreed. Clarified roles will allow DMPB to monitor task progress and will allow future program leads to identify areas for change to improve efficiency. Furthermore, updated documentation will provide additional clarity and improve tracking and reporting so that departmental leads are aware of, and taking responsibility and held accountable for, commitments and tasks.	• Map all internal and external stakeholders and their current roles; • Update the Workplan activities, RACI, Offices of Primary Interest and status; and • Communicate and validate roles and responsibilities with all stakeholders.	• Updated workplan and RACI to clarify roles and responsibilities for distribution to program stakeholders. • Confirmation by DG Steering Committee of updated documents.	December 2025	DMPB (until December 31, 2025) DOB (from January 1, 2026 onwards)
2. It is recommended that PSPC review, strengthen and finalize the risk management tools used by the CPSPC.	Agreed	• Review and update existing risk register and risk mitigation strategies (including integration of the risks identified in the Summer 2025 gap analysis) so as to re-baseline risks prior to	• Updated Risk Register for distribution to program stakeholders in alignment with program gap analysis. The updated Risk Register will reflect current status as well as to add ownership of	January 2026	DOB

Recommendations	Management Response	Management Action Plan	Deliverables	Targeted Implementation Date	Responsible
		starting initial phases of testing and implementation; • Strengthen the risk register and mitigation strategies by assigning ownership of risks to align with revised workplan and RACI (with each owner responsible to update risks and mitigation strategies as the program moves forward) and by including updated likelihood and impact assessments for all risks; and • Finalize the risk register and mitigation strategies through quarterly reviews with government and agency partners so risks and mitigations remain aligned with	risks to assist in the clarification of roles and responsibilities and will have revised likelihood and impact assessments. The revised risk register will include program risks, implementation risks, stakeholder risks, financial risks and legacy risks; • Confirmation by DG Steering Committee of updated documents to demonstrate acceptance and responsibility for revised risks; • Review of risk register with government agencies and partners and with the DG Steering Committee. DG review will include review of risk tolerance.		

Recommendations	Management Response	Management Action Plan	Deliverables	Targeted Implementation Date	Responsible
		program design and development. Quarterly presentation of key risks to the DG Steering Committee for discussion and consideration.			

Annex 2: Evaluation Methodology

Lines of evidence	Interviews	Document review	Surveys
METHODOLOGY	– **9 interviewed CPCSC stakeholders**: ▪ PSPC program management (DOB and DMPB): **5** ▪ PSPC working level (DOB and DMPB): **3** ▪ TBS (program management): **1**	– **~ 150 documents** reviewed ▪ ~ 50 CPCSC program planning documents ▪ ~ 20 CPCSC project management documents ▪ ~ 50 CPCSC governance documents including meeting minutes from various committees ▪ ~ 15 cyber security research documents ▪ ~ 10 CPCSC budget documents ▪ ~ 5 industry stakeholder engagement documents	– 33 surveys sent to CPCSC stakeholders across two separate surveys (working level and program management)
LIMITATIONS	– Close collaboration with DOB and DMPB allowed for most stakeholders of interest to be interviewed, presenting little limitation to data collection. – The client authority, DND, was not able to be interviewed.	– Close collaboration with DOB and DMPB allowed for all available documentation to be reviewed, presenting no limitation to data collection. – Documentation received was sufficient to formulate findings.	– Working level response rate: **11/21 (52%)** – Program management response rate: **5/12** (**42%)**
MITIGATION	– Evaluation preliminary findings and the draft final report were provided to the CPCSC Directors General Steering Committee for review as well as shared for review with the evaluation functions of partner departments.	– Not applicable	– When the same survey question was asked to both working-level and program management, responses were combined to include management's perspectives – Evaluation preliminary findings and the draft final report were provided to the CPCSC Directors General Steering Committee for review as well as shared for review with the evaluation functions of partner departments.