Public Safety Canada
Cyber Security Cooperation Program
Funding Application Guide

Call for Applications
August 7, 2019 – August 28, 2019
Introduction

This document is your step-by-step guide for information and guidance in completing an application for funding under the Cyber Security Cooperation Program (CSCP). It is meant to be used in tandem with the online application form.

Before applying:

Review the information in this Funding Application Guide carefully, noting all of the required information and supporting documentation. Please note that incomplete applications will not be considered for funding.

Should you have any questions about the application process, please contact the CSCP mailbox at CSCP-PCCS@ps-sp.gc.ca and a Program Officer will provide you with assistance.

Contents

This Funding Application Guide consists of six main sections and two annexes:

- **Section 1**: Program Overview
- **Section 2**: Application Requirements and Deadline
- **Section 3**: Call for Applications Information
- **Section 4**: Introduction to Building a Strong Application
- **Section 5**: Application Assessment Process
- **Section 6**: Contact Information

- **Annex A**: CSCP Terms and Conditions
- **Annex B**: CSCP Application Form Outline

**SECTION 1: PROGRAM OVERVIEW**

Public Safety Canada (the Department) is working to build a safe and resilient Canada through the CSCP, which provides time-limited funding in the form of grants and contributions. Funding under the CSCP supports projects that contribute to security and prosperity in the digital age while positioning Canada as a global leader in cyber security.

**CSCP Objectives**

The National Cyber Security Strategy, which articulates the Government of Canada’s vision for cyber security, has identified three key goals in consultation with stakeholders, the public and industry experts. These goals provide a focus for the activities and investments funded by the Government of Canada, in support of the Strategy’s vision.
<table>
<thead>
<tr>
<th>Goal</th>
<th>Objective</th>
</tr>
</thead>
</table>
| **Goal 1: Secure and Resilient Canadian Systems** | • Maintain and improve cyber security across all federal departments and agencies to protect the privacy of Canadians’ information held by the federal government, and the confidentiality, integrity, and availability of critical services for Canadians.  
• Enhance law enforcement capacity to respond to cybercrime.  
• Help support small and medium organizations in implementing cyber security regimes.  
• Consider how Canada’s advanced cyber capabilities could be applied to defend critical domestic networks and deter foreign cyber threat actors.  
• Work with provinces, territories, and the private sector to help define requirements to protect critical digital infrastructure. |
| **Goal 2: An Innovative and Adaptive Cyber Ecosystem** | • Work with partners to drive investment and foster cyber research and development. The Government will focus on emerging areas of Canadian expertise, such as quantum computing and blockchain technologies.  
• Explore initiatives to drive domestic demand for cyber security technologies and services.  
• Explore innovative and new ideas for making businesses and Canadians of all ages and backgrounds more cyber secure.  
• Work together across governments, academia, and the private sector to promote cyber workforce development and address the cyber skills gap.  
• Support Canadian research and statistics efforts to improve our collective understanding of cyber threats and opportunities. |
| **Goal 3: Effective Leadership, Governance and Collaboration** | • Streamline the way the Government of Canada works and collaborates with external partners and stakeholders by establishing a clear focal point for authoritative advice, guidance, and cyber incident response.  
• Reinvigorate public awareness and engagement efforts and establish new forums for collaboration.  
• Lead, in partnership with provinces, territories, and the private sector, the development of a national plan to prevent, mitigate and respond to cyber incidents.  
• Work with international partners to advance Canadian interests. This includes advocating for an open, free, and secure internet and enhancing our international cooperation to combat cybercrime. |
Eligible Recipients

Financial assistance may be provided to the following classes of recipients:

- Canadian not-for-profit organizations;
- Canadian academic and research institutions;
- Provincial, territorial and local government and authorities;
- Canadian individual researchers and professionals; and
- Canadian for-profit organizations.

For full information on recipient eligibility, please refer to the CSCP Terms and Conditions (Annex A).

Eligible Expenditures

Funds may only be used for eligible expenditures that have been identified in a budget approved by the Department. Eligible expenditures will be those that are incurred by the Recipient, are reasonable, incremental, directly related to, and required to carry out the project activities.

Eligible expenses include:

a) salaries and wages for permanent or temporary professional, clerical, technical and administrative services, and stipends (including expenses for international staff);
b) consultation fees, and audit fees;
c) training or educational fees (e.g. courses, workshops, etc.);
d) conference room and meeting room rentals;
e) office equipment and minor capital acquisitions net of disposal (less than $5,000 per acquisition);
f) reasonable travel and living expenses related to the delivery of the project, including transportation rental fees;
g) honoraria, defined as time limited remuneration for a volunteer service or participation in project delivery that is consistent with, and essential to the attainment of, the project’s objectives;
h) computer services, library expenses, research costs and collection and analysis of statistics;
i) public awareness and educational activities consistent with the project’s objectives;
j) translation and simultaneous interpretation activities;
k) hospitality (meals and refreshments), only in the context of research projects where focus groups are undertaken;
l) shipping charges, postage, licenses, and other fees; and,
m) federal and provincial taxes (only after credits and reimbursements have been considered).
Other eligible expenses:

Administrative & overhead costs which may not be explicitly incurred for the purpose of the delivery of the project, but enable its achievement, could be considered as other eligible expenses. These costs may not be effectively tracked to the project. Therefore, they will be apportioned to the project based on a reasonable methodology predefined in writing by the Recipient, in the budget request. Combined, these expenses should not exceed 15% of the total eligible project costs funded by the Department.

The nature of these costs should not be covered under any of the other above categories. They may include:
   a) office supplies;
   b) printing;
   c) publishing;
   d) distribution; and,
   e) promotion.

For more detailed information about eligible expenses, please refer to the Budget template, or CSCP Terms and Conditions (Annex A).

SECTION 2: APPLICATION REQUIREMENTS AND DEADLINE

The current call for applications is open from August 7, 2019 to August 28, 2019. Completed applications must be submitted online no later than 11:59 Pacific Time (PDT) on August 28, 2019.

All applicants will receive a confirmation email that their submission was received. If a confirmation email is not received after submission please contact the CSCP mailbox at CSCP-PCCS@ps-sp.gc.ca for assistance.

To be considered for funding, an application must include a completed:

1. Online Funding Application Form (mandatory);
2. Project Budget Template (mandatory); and,
3. Project Workplan Template (mandatory).

Applicants must use the official templates provided on the CSCP webpage to be considered eligible.

Incomplete applications and applications received after 11:59pm Pacific Time (PDT) - August 28, 2019 will not be considered for funding.
### 1. Security and Resilience

- Research and development of new technologies and tools for increasing the security and resilience of Canadian cyber systems, including for the prevention, mitigation and/or response to cyber-attacks;
- Development and dissemination of knowledge products, training or best practices aimed at increasing stakeholders’ understanding of technological advancements, cyber threats and vulnerabilities; and,
- Support for non-federal partners’ implementing actions to better protect their systems and information.

### 2. Cyber Innovation

- Research and development of innovative cyber security tools, products and solutions, including for addressing threats posed by disruptive and emerging technologies (e.g., Internet of Things, Smart Cities, Fintech, quantum computing, etc.);
- Academic research to expand the cyber knowledge base, with a view to help identify and anticipate upcoming trends, domestic and/or international;
- Support for training and other educational programs to advance cyber security skills and knowledge, and increase the number of cyber security professionals in the Canadian workforce. The projects could include:
  - Workshops, colloquiums, conferences and other educational forums and programs;
  - Development and disseminations of materials to support training and education; and,
  - Other projects promoting Science, Technology, Engineering, and Mathematics (STEM), arts, and business fields across all levels of education.
- Increase the availability and access of cyber innovations, including through the commercialization of new technologies.

### 3. Effective Leadership

- Projects and initiatives that aim to increase public awareness of cyber threats, such as public awareness campaigns or other communication activities;
- Projects and initiatives to generate/gather metrics and data to support decision-making, such as the production and analysis of data; and,
- Projects and initiatives that promote collaboration and the exchange of information and knowledge among multiple stakeholders and critical infrastructure sectors.

### Maximum Funding per Project

- Maximum funding shall not exceed $300,000/year per Contribution or Grant.
- In the case of for-profit organizations, the maximum funding is set at $100,000/year per Contribution; and $150,000/year per Grant. Applications eligible for funding as a Grant will be determined by the Selection Committee and CSCP Terms and Conditions (annex A).
Stacking Requirement

- Total Canadian Government funding (federal/provincial/territorial/municipal) does not exceed 75% of the total eligible expenditures.
- Funding agreement may be in the form of multi-year funding. No project will extend beyond March 31, 2024.

SECTION 4: INTRODUCTION TO BUILDING A STRONG APPLICATION

To build a strong application, the applicant needs to make sure the following key elements are addressed in the application:

- Use simple language. Only use jargon when necessary. Character limits in the application range from 1000 to 2500 characters;
- Identify your project objectives, ongoing actions, and deliverables, and how they each flow into each other;
- Communicate the intended results of the project clearly;
- Demonstrate how your project and initiative provides advice and/or policy recommendations to the Government of Canada;
- Consider collaborating with other individuals/groups/networks/alliances during or after the project is complete in order to enhance long-term impact of the results and deliverables; and,
- Draft a strong budget and work plan for your project.

There are a number of resources available that provide guidance on developing applications for a project for advancing cyber security in Canada that are valuable to consider. Applicants are encouraged to explore the following resources:

- Cyber Security Action Plan: Budget 2018 Investments
- Gender-Based Analysis Plus – Government of Canada’s Approach

SECTION 5: APPLICATION ASSESSMENT PROCESS

Assessment Criteria

Eligible applications will undergo a criteria-based assessment process to ensure that all project applications are assessed objectively against the same criteria, the CSCP Terms and Conditions, and the availability of funding.
Assessment Process

The project assessment process will consist of:

- Initial review to verify that mandatory information has been provided, and basic eligibility criteria are met (see Annex A for basic eligibility of recipient and activities);
- Detailed review to assess the project against merit criteria; and,
- Review by a Selection Committee, made up of officials from federal departments and agencies responsible for cyber security.

Communication of Results

Results of the open call process will be communicated to applicants by no later than November 30, 2019.

Selected projects could start as early as December 2019.

SECTION 6: CONTACT INFORMATION

Please direct requests for assistance to the CSCP mailbox at CSCP-PCCS@ps-sp.gc.ca. Program Officers are available to provide advice on the eligibility of applicants, activities and expenses and to answer general questions. Please note that completed applications will not be reviewed prior to submission.

For additional information on the CSCP, please refer to the CSCP website.
ANNEX A

Terms and Conditions for Grants and Contributions
under the Cyber Security Cooperation Program

1.0 Authority

The Minister’s authority to make transfer payments is provided for by section 6(1)(c) of the
Department of Public Safety and Emergency Preparedness Act, S.C. 2005, ch.10. It provides that the
Minister of Public Safety and Emergency Preparedness may, in exercising his or her powers and in
performing his or her duties and functions, and with due regard to the powers conferred on the
provinces and territories, make grants or contributions.

Sections 4(1)(m), (o), (p) and (q) of the Emergency Management Act assigns responsibility to the
Minister for such things as promoting the adoption of standards and best practices and the conduct
of research with respect to emergency management while section 6(1) assigns responsibility to the
Minister to identify the risks that are within or related to his area of responsibility.

2.0 Purpose

The Department of Public Safety and Emergency Preparedness’s (the Department) Cyber Security
Cooperation Program (CSCP) aims to contribute to the federal government’s leadership role in
advancing cyber security in Canada. By enabling close collaboration with other levels of governments,
the private sector, academia, and non-governmental organizations, the CSCP’s purpose will be to
commission research and yield comprehensive results that help position Canadian governments,
businesses, and citizens to better anticipate trends, adapt to a changing environment, and remain on
the leading edge of innovation in cyber security.

3.0 Duration

The current terms and conditions for the CSCP will be valid from the date they receive approval from
the Treasury Board Secretariat until March 31, 2024.

4.0 Objectives

In alignment with the goals and priorities of the new National Cyber Security Strategy (NCSS), the
CSCP is comprised of the following three streams and related objectives:

1. **Security and Resilience**: The number and complexity of cyber threats continues to increase.
The goal of this stream is to incentivize research and action in the area of cyber resilience. This
includes projects that aim to encourage national action to bolster the security and resilience
of Canadian systems to cyber threats, and to increase the national cyber security baseline
across the country. Funding will be provided for projects that enhance the capacity to
prevent, mitigate, and respond to advanced cyber attacks targeting Canadian systems and
institutions, and help defend critical government and private sector systems. This includes
supporting activities that not only encourage and assist non-federal partners to better protect themselves, but also ensure that Canadian cyber systems are prepared for and can take advantage of rapid technological advancements.

2. **Cyber Innovation:** Canada will need to develop innovative cyber security tools and areas of cyber specialization if it is to remain at the forefront of emerging technology and raise a new generation of connected, cyber-capable Canadians. The goal of this stream is to position Canada to take advantage of the economic benefits that can derive from innovations in the cyber security field. Funding will be provided for projects that assist Canadian governments, businesses and citizens in anticipating trends, and that address emerging threats to cyber security posed by disruptive and emerging technologies. This includes support for advanced research and development, and for projects that advance cyber security skills and knowledge in Canada.

3. **Effective Leadership:** Canada’s success in cyber security will depend on multiple actors working together on complex and evolving issues. The goal of this stream is for the Government to demonstrate leadership and promote national coordinated action to advance cyber security knowledge, skills and innovation in Canada. Funding will be provided to support projects that enhance stakeholders’ collaboration and coordination in increasing the body of knowledge and understanding of cyber security issues, and ensure that Canadian values and interests are strengthened, preserved and defended. This includes projects that increase public awareness of cyber threats, as well as projects that begin to address the fundamental gap in available current Canadian data and metrics related to cyber security, with a view to improve decision-making.

### 5.0 Expected Results / Performance Measurement Strategy

The CSCP contributes to the achievement of departmental and governmental objectives of building a safe and resilient Canada, and enhancing Canada’s resilience to cyber events and incidents. It falls under section 1.1 (National Security) and section 1.1.3 (Cyber Security) of the Department’s Program Inventory.

The CSCP plays a critical role in working towards the expected outcomes and goals of the new “National Cyber Security Strategy: Canada’s Vision of Security and Prosperity in the Digital Age”. It aims to help Canada address evolving cyber threats, realize the economic benefits of cyber security and enhance national collaboration and engagement of stakeholders.

<table>
<thead>
<tr>
<th>Expected Results</th>
<th>Key performance measures and indicators</th>
</tr>
</thead>
<tbody>
<tr>
<td>The understanding of cyber vulnerabilities and threats is enhanced among stakeholders.</td>
<td>Percentage of stakeholders that indicate having an increased awareness of cyber threats and vulnerabilities.</td>
</tr>
<tr>
<td>Research funded through the CSCP helps to ensure that the Department’s decision making is evidence-based.</td>
<td>Percentage of CSCP research projects cited in National Cyber Security Directorate (NCSD) policy and guidance documents.</td>
</tr>
</tbody>
</table>
11

<table>
<thead>
<tr>
<th>Expected Results</th>
<th>Key performance measures and indicators</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-federal Canadian systems and information are less vulnerable and better secured against cyber threats.</td>
<td>Percentage of stakeholders that indicate an overall improvement of their cyber security posture.</td>
</tr>
<tr>
<td></td>
<td>Percentage of stakeholders that indicate that they are adopting cyber best practices.</td>
</tr>
</tbody>
</table>

The Department will draw on the horizontal performance measurement strategy for the NCSS, to ensure that appropriate indicators are established and to promote an effective evaluation of the program.

6.0 Eligible Recipients

Grants and Contributions may be provided to the following classes of Recipients:

   a)  Canadian not-for-profit organizations;
   b)  Canadian academic and research institutions;
   c)  Provincial, territorial and local governments and authorities; and,
   d)  Canadian individual researchers and professionals.

In addition to the above list, Contributions may also be provided to the following class of Recipients:

   a)  Canadian for-profit organizations.

7.0 Nature and Type of Eligible Initiatives or Projects

The nature and type of initiatives or projects that are considered eligible for funding must be aligned with the objectives of one of the CSCP’s three streams, as listed under Section 3.0 of the current Terms and Conditions document. They may include the following:

<table>
<thead>
<tr>
<th>Stream</th>
<th>Potential Initiatives or Projects Eligible for Funding</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security and Resilience</td>
<td>•  Research and development of new technologies and tools for increasing the security and resilience of Canadian cyber systems, including for the prevention, mitigation and/or response to cyber attacks.</td>
</tr>
<tr>
<td></td>
<td>•  Development and dissemination of knowledge products, training or best practices aimed at increasing stakeholders’ understanding of technological advancements, cyber threats and vulnerabilities.</td>
</tr>
<tr>
<td></td>
<td>•  Support for non-federal partners’ implementing actions to better protect their systems and information.</td>
</tr>
<tr>
<td>Stream</td>
<td>Potential Initiatives or Projects Eligible for Funding</td>
</tr>
<tr>
<td>----------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Cyber Innovation</td>
<td>• Research and development of innovative cyber security tools, products and solutions, including for addressing threats posed by disruptive and emerging technologies (e.g., Internet of Things, Smart Cities, Fintech, quantum computing, etc).</td>
</tr>
<tr>
<td></td>
<td>• Academic research to expand the cyber knowledge base, with a view to help identify and anticipate upcoming trends.</td>
</tr>
<tr>
<td></td>
<td>• Support for training and other educational programs to advance cyber security skills and knowledge, and increase the number of cyber security professionals in the Canadian workforce. These projects could include:</td>
</tr>
<tr>
<td></td>
<td>o Workshops, colloquiums, conferences and other educational forums and programs.</td>
</tr>
<tr>
<td></td>
<td>o Development and dissemination of materials to support training and education.</td>
</tr>
<tr>
<td></td>
<td>o Other projects promoting STEM (science, technology, engineering, mathematics) fields across all levels of education.</td>
</tr>
<tr>
<td></td>
<td>• Increase the availability and access of cyber innovations, including through the commercialization of new technologies.</td>
</tr>
<tr>
<td>Effective Leadership</td>
<td>• Projects and initiatives that aim to increase public awareness of cyber threats, such as public awareness campaigns or other communication activities.</td>
</tr>
<tr>
<td></td>
<td>• Projects and initiatives to generate/gather metrics and data to support decision-making, such as the production and analysis of datasets.</td>
</tr>
<tr>
<td></td>
<td>• Projects and initiatives that promote collaboration and the exchange of information and knowledge among multiple stakeholders.</td>
</tr>
</tbody>
</table>

### 8.0 Eligible Expenditures

Funds may only be used for eligible expenditures that have been identified in a budget approved by the Department. Eligible expenditures will be those that are incurred by the Recipient, are reasonable, incremental, directly related to, and required to carry out the project activities.

Eligible expenses include:

a) salaries and wages for permanent or temporary professional, clerical, technical and administrative services, and stipends (including expenses for international staff);

b) consultation fees, and audit fees;

c) training or educational fees (e.g. courses, workshops, etc.);

d) conference room and meeting room rentals;

e) office equipment and minor capital acquisitions net of disposal (less than $5,000 per acquisition);
f) reasonable travel and living expenses related to the delivery of the project, including transportation rental fees;
g) honoraria, defined as time limited remuneration for a volunteer service or participation in project delivery that is consistent with, and essential to the attainment of, the project’s objectives;
h) computer services, library expenses, research costs and collection and analysis of statistics;
i) public awareness and educational activities consistent with the project’s objectives;
j) translation and simultaneous interpretation activities;
k) hospitality (meals and refreshments), only in the context of research projects where focus groups are undertaken;
l) shipping charges, postage, licenses, and other fees; and,
m) federal and provincial taxes (only after credits and reimbursements have been considered).

Other eligible expenses:

Administrative & overhead costs which may not be explicitly incurred for the purpose of the delivery of the project, but enable its achievement, could be considered as other eligible expenses. These costs may not be effectively tracked to the project. Therefore, they will be apportioned to the project based on a reasonable methodology predefined in writing by the Recipient, in the budget request submitted at the onset of the agreement. Combined, these expenses should not exceed 15% of the total eligible project costs funded by the Department.

The nature of these costs should not be covered under any of the other above categories. They may include:

   a) office supplies;
   b) printing;
   c) publishing;
   d) distribution; and,
   e) promotion.

Ineligible expenses:

   a) capital costs, such as land, buildings, vehicles and most other major capital costs (more than $5,000 per acquisition);
   b) hospitality (meals, beverages or refreshments, and entertainment);*
   c) rent, normal utilities such as electricity, heat, water and telephone, maintenance of offices and other buildings, insurance and taxes; and,
   d) contributions to Employment Insurance, the Canada Pension Plan, the Workers’ Compensation Board, the Provincial Pension Plan or other Employee Benefit Plans.

*Food and refreshment may be considered eligible costs in the context of research projects where focus groups are undertaken.
9.0 Maximum Amount Payable and Period

Funding amounts will be determined based on an assessment of the Recipient’s planned activities and budget submission, previous financial performance, and capacity of the Recipient to achieve results. The CSCP’s review authorities will also take into consideration similar projects and other sources of funding. Assistance will be provided at the minimum level required to ensure the project can proceed within the proposed time, location and scope, and to further the CSCP’s objectives and expected results. Any contributions made to for-profit organizations are not intended to allow the business to generate profits or to increase the value of the business.

The maximum amount of financial assistance payable to each Recipient will be limited by the Vote appropriated for this purpose, the availability of the CSCP funds and the number of successful applicants. The maximum funding amount shall not exceed $300,000 annually per Contribution. In the case of for-profit organizations, the maximum funding amount shall not exceed $100,000 annually per Contribution. The maximum funding amount shall not exceed $150,000 annually per Grant.

Funding agreements may be in the form of multi-year funding. No project will extend beyond March 31, 2024.

10.0 Stacking Limit

The Department will ensure that contributions made under the funding program do not cover expenses already covered through another funding program or strategy. To that effect, Applicants/Recipients will be required to disclose all confirmed and potential sources of funding (governmental and non-governmental) for a proposed project, before the start and at the end of a project.

Where possible and appropriate, the cost of an eligible activity will be shared between the Department, the Recipient and/or external funders. The Department will ensure that the total Canadian government funding (federal/provincial/territorial/municipal assistance) does not exceed 75% of the total eligible expenditures.

11.0 Method of Payment

Grants:

Payments will be issued in the form of instalments, unless the full amount is required in a single payment to meet the objectives of the grant.

Payments can be made up to a portion of the grant amount prior to completion of the project, as determined by an assessed level of risk.

Recipients must meet, and continue to meet, the specific Terms and Conditions of the Grant Agreement, prior to payments being made.
Contributions:

Payments for contributions, including advance payments, will be issued to Recipients pursuant to the provisions of the Treasury Board Policy on Transfer Payments and based on the reimbursement of eligible expenditures. Payments can be made up to a portion of the contribution amount, based on a cash flow requirement and on a Risk Assessment of the Recipient. The assessed level of risk will also determine requirements for a holdback provision to be included in the Agreement.

Progress payments will be issued to reimburse the Recipient for expenditures made. They will be based upon receipt and acceptance by the Department of interim financial and non-financial project reports outlining the activities and expenditures to date.

Where advance payments are required for the successful implementation of the project, they will be issued in accordance with the Recipient’s cash flow requirements and the Agreement’s risk profile.

Recipients must meet, and continue to meet, the specific Terms and Conditions of the Contribution Agreement, prior to payments being made.

Provided that the recipient has met the Terms and Conditions of the Contribution Agreement, a final payment will be made only upon receipt and acceptance of a final financial statement covering the duration of the project. When deemed necessary by the Risk Assessment, audited financial reports will be requested for the project.

12.0 Application Process and Requirements

A Call for Proposals (CFP) will be issued up to twice per fiscal year. Each CFP will be posted on the CSCP website for a duration of three weeks and will lay out the specific application requirements, such as the necessary forms and guidelines.

For the Department to consider a project proposal, all applicants will be required to provide the following supporting material:

- A detailed project description, including a description of the proposed activities, the anticipated reach, and expected results (desired outcomes) of the project. These must relate to the objectives and key expected results of the CSCP.
- The amount of funding requested under the CSCP.
- An itemized budget for the entire project, disclosing all revenues from all sources (confirmed and potential). This should include in-kind support, as well as every expenses expected over the life of the project.
- Names, titles and contact information of the persons responsible for managing the project.
- A commitment to provide a report on the results.
Depending on the nature and duration of the project, the following additional supporting material could be requested:

- An implementation plan, including a description of the targeted clientele, the expected outputs and outcomes, the data gathering methodologies and timelines.
- A copy of the beneficiary’s most recent applicable financial statements.

In addition, to prevent the risk of conflict of interest, the recipient must:

- Disclose the involvement of prospective recipients who are subject to the *Values and Ethics Code for the Public Service*, the *Conflict of Interest Act* (S.C. 2006, C.9) or the *Parliament of Canada Act* (R.S., 1985, c. P-1.01).
- When required by the *Lobbying Act*, register lobbyists under the *Lobbying Act* (applicants shall provide assurance that, where lobbyists are utilized, they are registered in accordance with the *Lobbying Act* and that no actual or potential conflict of interest exists nor any contingency fee arrangement).
- Discuss the role of a departmental official, if one is to participate on an advisory committee or board. Such involvement must not be seen to be exercising control on the committee or board, or on the use of the funds.

Unsolicited proposals submitted outside of the official Call for Proposals timeframe could be considered, at the discretion of the CSCP. In such cases, Applicants should consult the CSCP to discuss their project prior to submitting a completed application.

**13.0 Review Process and Assessment Criteria**

Proposals for consideration under the CSCP will be reviewed against program criteria by the selection committee. The selection committee will be chaired by the Director General, National Cyber Security Directorate (NCSD) or their delegate, and made up of officials from federal departments and agencies responsible for cyber security, appointed to the selection committee by the Department’s Senior Assistant Deputy Minister, National Security.

In reviewing the eligibility of Recipients for grants, NCSD will use the following criteria:

- The recipient must be a not-for-profit organization.
- The resources funding required to deliver on the proposal can be identified and validated during the review process and the expected results can be adequately and most effectively demonstrated through the use of activity/performance reporting.
- The level of risk must be low, as assessed through:
  - The total budgetary allocation of the Agreement.
  - The ability of the Applicant to develop, implement, manage, monitor, document and evaluate activities within the specified timeframe and budget.
  - The Department’s previous experience working with the Applicant, the degree of collaboration and the quality of and success of the project(s).
The activities outlined in the Agreement and the difficulty associated with achieving the desired objectives.

Arrangements that exists for the Agreement in terms of the type of partners, the experiences of the Recipients with these partners, and the confirmation from partners.

The degree to which the Agreement may withstand public scrutiny.

In reviewing and recommending proposals, NCSD will take into consideration, as applicable and appropriate:

- The extent to which the project would directly support and advance the objectives of the relevant stream of the CSCP, as stated in this document.
- The extent to which the outcomes of the project can be leveraged in subsequent work.
- The extent to which it is demonstrated that the proposed project is evidence based and could strengthen Canada’s cyber security.
- The extent to which the project complements the work of the Department or other Government Department’s efforts, including the National Cybercrime Coordination Unit and the Canadian Centre for Cyber Security.
- The amount of funding requested relative to the amount of resources available from the Department in any given year, and whether expenses outlined in the proposal are eligible and reasonable.
- The ability of the applicant to develop, implement, manage, monitor, document and evaluate activities within the specified timeframe and budget.
- The Department’s previous experience in working with the applicant – the applicant’s degree of involvement and collaboration, the quality of the project and its success.
- The project’s potential for portability and for building on the existing knowledge base as related to Canada’s cyber security.
- The type, extent and distribution plans for report(s) or other material produced.
- The ethical implications of the project.
- The level of support for the proposal from relevant communities, provincial/territorial governments, federal departments and agencies, other stakeholders and partners relevant to the project.
- Whether the applicant occupies a credible and strategic position relevant to cyber security for the purpose of the project/initiative.
- Whether the proposal includes a plan for monitoring, regular reporting, evaluation and dissemination.

In reviewing and recommending proposals, NCSD will have evaluation criteria for each call for proposals and category. In addition to the eligibility criteria and priorities identified under each stream, applications will be assessed on their merit, level of risk, and alignment with the program objectives.
14.0 Monitoring and Reporting

Grants:

Recipients will be required to report on results achieved, to support the CSCP’s performance measurement strategy and departmental reporting. Specific reporting requirements will be included within each Grant Agreement.

Contributions:

A schedule of reporting requirements will be included within each Contribution Agreement.

Recipients are required to provide the Department with reports outlining the activities undertaken in support of their approved project. Reports are to include the results to be achieved with the funding provided under the CSCP, and the methods used. In addition, Recipients will be required to provide detailed financial reports outlining the costs incurred in relation to their approved project, including a final accounting of eligible expenditures.

Based on an assessed level of risk as identified by Recipients and assessed by the Department’s internal review committee, Recipients may be required to provide the Department with an update on progress towards eligible activities, as deemed necessary. This will be used for monitoring and reporting purposes, to determine whether objectives and targets are being (or are likely to be) met.

15.0 Official Languages

The Department will work with Applicants/Recipients in their preferred official language. All material and information related to the program will be made available by the Department in both official languages.

The Recipients’ communication with, and delivery of services or benefits to the public will be made available in both official languages, in accordance with the Official Languages Act and the Treasury Board’s policies and directives on official languages.

16.0 Intellectual Property

If a project produces intellectual property, the Recipient retains copyright of any work produced under the Contribution Agreement. However, in situations where the Department wishes to use the intellectual property produced by a Recipient, additional clauses may be included in the Contribution Agreement or the Department may negotiate a licence with the Recipient.
ANNEX B

CSCP Application Form Outline

Contact Information
Organization's legal name
Organization address
Primary contact for the project
Signing authority for the project

Project Overview
Project Title
Project Location(s)
Project Duration (months)
Total Project Cost (CAD$)
Public Safety Canada Funding (CAD$)
Total Public Safety Canada Funding in First Year (CAD$)

Funding Stream (select one)

Security & Resilience (select all eligible initiatives that apply)
Cyber Innovation (select all eligible initiatives that apply)
Effective Leaderships (select all eligible initiatives that apply)

Section 1: Applicant Organization

Q1.1 Type of organization (select one)

Q1.2 Describe the expertise, resources, skills, experience and knowledge that qualify your organization to deliver this project (3000 character limit)

Q1.3 Please provide information regarding the organization's previous history of managing project budgets (2500 character limit)

Section 2: Project Information

Q2.1 Brief description of the project (2500 character limit)
A brief description of the overall purpose, objectives, and scope of the project.

Q2.2 Describe the links between the project activities and deliverables (2500 character limit)
Referencing the Project Workplan document, as well as evidence from the demonstrated need, describe how and why the activities listed link to the anticipated deliverables.

Q2.3 Describe how your project will support and advance the CSCP program objectives (2500 character limit)
Describe the linkages the project has to the CSCP objectives as found in the Terms and Conditions of the program.

Q2.4 Demonstrate the need for the project (2500 character limit)
Describe the nature and extent of the priority issue to be addressed by the project, including empirical evidence and sources of that evidence where possible, to establish a clear need for the project.

Q2.5 Identify and describe the projects cross-sectoral collaboration and partnerships (2500 character limit)
Identify and describe cross-sectoral collaboration and partnerships within or outside of your jurisdiction. If no partnerships exist, demonstrate how you will seek to increase collaboration through the duration of the project.

Q2.6 Describe the project risk and mitigation strategy (2000 character limit)
Identify any potential project risks. If no risks are identified, provide a rationale to demonstrate the project has no potential risks. If risks are identified, analyze their potential impact, and identify the measures that will be implemented to mitigate the risk.

Q2.7 Describe the anticipated impact of the project (2500 character limit)
Describe the anticipated and/or potential contribution to academic knowledge, and/or to the knowledge and capabilities of relevant users such as practitioners, policymakers and the general public.

Gender-Based Plus Analysis (GBA+)
Gender-based Analysis Plus (GBA+) is an analytical process used to better understand the different types of experiences and needs of diverse individuals and groups, in order to enhance the success and reduce potential harms of policies, programs, and research projects. Diversity in this context may refer to categories such as sex, gender, race, ethnicity, religion, age, geographic location, socio-economic status, and mental or physical disability, as appropriate to the project.

Does your overall project design consider a diverse range of individuals and/or groups? (Yes/No)

If yes, please explain how your overall project design considers diversity. If not, please provide a brief rationale for why it is not applicable. Indicate data sources and/or evidence that were considered to support this conclusion. (1000 character limit)

Does your project design specifically address any diversity considerations? (Yes/No)

If yes, please explain how your project design addresses any specific consideration(s). If not, please provide a brief rationale for why it is not applicable. (1000 character limit)

Will data collected through your project likely be broken down into categories to help understand its impact on diverse individuals and/or groups? (Yes/No)

If yes, please provide and explain the expected categories to be used. If not, please provide a brief rationale for why it is not applicable. (1000 character limit)

Budget Upload Link

Workplan Upload Link