Innovation, Science and Economic Development Canada
Innovation, Sciences et Développement économique Canada

Canada

CYBER SECURITY INNOVATION NETWORK PROGRAM

This publication is available online at https://www.ic.gc.ca/eic/site/149.nsf/eng/h_00000.html

To obtain a copy of this publication, or to receive it in an accessible format (Braille, large print, etc.), please fill out the Publication Request Form at www.ic.gc.ca/Publication-Request or contact:

ISED Citizen Services Centre
Innovation, Science and Economic Development Canada
C.D. Howe Building
235 Queen Street
Ottawa, ON K1A 0H5
Canada

Telephone (toll-free in Canada): 1-800-328-6189
Telephone (international): 613-954-5031
TTY (for hearing impaired): 1-866-694-8389

Business hours: 8:30 a.m. to 5:00 p.m. (Eastern Time)

Email: ISED@canada.ca

Cat. No. Iu37-30/2021E-PDF
ISBN 978-0-660-37904-3

Aussi offert en français sous le titre *Réseau d’innovation pour la cybersécurité*

Table of contents

1. Introduction to the Cyber Security Innovation Network

1.1 Context

Budget 2019 announced an investment of $80 million over four years to support three or more Canadian centres of expertise on cyber security across Canada affiliated with post-secondary institutions. The intent of the Cyber Security Innovation Network Program is to fund a national cyber security network to be led by Canadian centres of expertise on cyber security affiliated with post-secondary institutions, with a minimum of three participating centres of expertise, in collaboration with private sector and other partners. The network must be pan-Canadian and will enhance research and development (R&D), increase commercialization, and develop a pipeline of skilled cyber security talent across Canada.

Innovation, Science and Economic Development Canada (ISED) is seeking to enter a four-year, non-repayable contribution agreement with a selected applicant who will form the Cyber Security Innovation Network. The value of the contribution agreement will be up to $80 million over four years (2021-22 to 2024-25).

This program guide provides information on the program's objectives, eligibility and assessment criteria, expected outcomes, and details about how to apply.

1.2 Vision, mission, and objectives of the Cyber Security Innovation Network

Vision: To support a national network to grow Canada's cyber security ecosystem through academic-industry collaboration.

Mission: The Cyber Security Innovation Network will seek to enhance and expand cyber security research and development; increase commercialization; and, develop a pipeline of skilled cyber security talent.

Objectives:

- The network will support research and development in cyber security by encouraging collaboration between Canada's post-secondary institutions, the private sector, and other partners in order to accelerate the development of innovative cyber security products and/or services;
- The network will seek to accelerate the commercialization of cyber security products, services and/or processes that enter the marketplace; and,
- The network will seek to diversify, deepen and expand Canada's cyber security pipeline of talent, including the recruitment and retention of faculty, trainers, and instructors, and by providing more resources to curriculum development, training, reskilling and upskilling of the cyber security workforce through initiatives designed and delivered in collaboration with industry partners.

2. Program requirements

2.1 Eligibility criteria

To become eligible under the Cyber Security Innovation Network program, an applicant must meet all of the following criteria in their proposal:

- Be comprised as a network to be led by three or more Canadian centres of expertise on cyber security affiliated with post-secondary institutions;
  - A centre is defined as an organization affiliated with a recognized Canadian post-secondary institution that supports the growth of the cyber security innovation ecosystem.

- Be federally incorporated as a not-for-profit organization under the *Canada Not-for-Profit Corporations Act* (not required to be incorporated at the time of application);

- Be representative of the diversity of Canada's cyber security ecosystem. The following categories of partners are expected to be included in the network proposal (but are not limited to):
  - centres of expertise on cyber security affiliated with post-secondary institutions (other than the centres coming forward as applicants);
  - private sector (including both small and medium sized enterprises (SMEs) and larger enterprises);
  - Canadian post-secondary institutions (e.g., research centres, universities, colleges, polytechnics);
  - not-for-profit organizations (e.g., industry associations, incubators and accelerators, skills development organizations, etc.); and,
  - provincial/territorial/municipal governments.

- Include commitments from a combination of partners to match the funds requested of the Cyber Security Innovation Network program at a 1:1 ratio (see section 2.9 Matching fund requirements for further details);

- Be pan-Canadian. This is defined as including centres of expertise on cyber security affiliated with post-secondary institutions and partners from across Canada's regions (Western/Northern Canada, Central (with representation from both Ontario and Quebec) and Atlantic Canada); and,

- Demonstrate a national vision for the network to advance cyber security research and development, commercialization, and skills and talent development activities that reflect areas of cyber security needs and specialization across Canada.

Network model

Lead recipient

Following the signature of a contribution agreement, the applicant will be referred to as a "lead recipient". The lead recipient must be a not-for-profit organization, incorporated under the *Canada Not-For-Profit Corporations Act*, prior to the signing of a contribution agreement. The lead recipient will be the body responsible for implementing the strategic direction of the network to achieve the objectives of the Cyber Security Innovation Network program and for the administration and redistribution of the federal contribution.

The lead recipient will be required to administer its own operations. ISED will not play an operational role in the implementation of activities or the management of relationships between organizations involved in the proposed network.

Ultimate recipients

The lead recipient may distribute funds to ultimate recipients, to fulfill the eligible activities that will be outlined in a contribution agreement (see section 2.3 on Eligible activities for further details). The lead recipient is expected to enter into legally binding funding agreements with ultimate recipients and monitor their compliance against the contribution agreement's terms, conditions and obligations, to track progress and ensure accountability for use of funds.

Examples of ultimate recipients in a network may include organizations that will:

- contribute to the cost-matching requirement of the program and carry-out project activities; and,
- carry-out project activities and not contribute to the cost-matching requirements (e.g., ultimate recipients could be selected as a result of a call for proposals and receive network funding only).

Types of organizations eligible to become ultimate recipients may include:

- centres of expertise on cyber security affiliated with post-secondary institutions (other than the centres coming forward as applicants);
- private sector (including both small and medium sized enterprises and larger enterprises);
- Canadian post-secondary institutions (e.g., research centres, universities, colleges, polytechnics); and,
- not-for-profit organizations (e.g., industry associations, incubators and accelerators, skills development organizations, etc.).

2.2 Governance structure and management

The lead recipient must put in place governance and administrative structures to support the activities of the network. Applicants must demonstrate how they intend to put in place the following network governance requirements.

Board of directors

In accordance with the creation of a federal not-for-profit entity, the network must appoint a governing Board that has the overall responsibility for the governance and management of the Cyber Security Innovation Network. The Board of directors will be responsible for the network's management, strategic direction, and financial accountability, as well as the execution of the network's annual corporate plan and the approval of the annual report and audited financial statements.

Private sector involvement (including SMEs and larger enterprises) on the Board of directors and governance structure of the network is expected. Participation is expected to be diverse, inclusive, gender balanced, and pan-Canadian. The composition of the permanent Board of directors must strive to meet a gender parity representation target of 50 percent, and a 30 percent target for participation from other underrepresented groups. (see section 2.8 Equity, diversity, and inclusion framework for further details).

Key management positions

At a minimum, the management structure of the network must include the following three positions:

	Position	Description
1.	**Chief Executive Officer**	The network must appoint a Chief Executive Officer who reports to the Board of directors. The executive officer will be responsible for the operations of the network.
2.	**Chief Information Security Officer**	The network must identify a Chief Information Security Officer who will be responsible for leading the implementation of the network's data management strategy and cyber security plan. See sections 2.4 Cyber security plan and 2.5 Data management strategy for further details.
3.	**Chief Financial Officer**	The network must identify a Chief Financial Officer responsible for the management of the network's financial affairs.

Network staff

The network must put in place operational staff responsible for the delivery of network operational activities, including, but not limited to, the redistribution of program funds, internal projects, and partnerships. Operational staff will also be responsible for liaising with ISED and for preparing documentation associated with the network's reporting requirements under the contribution agreement (see section 5. Oversight and monitoring for further details).

The network will be encouraged to identify key roles that will support the delivery of network operations. Examples of positions include, but are not limited to:

- human resources officer;
- equity, diversity, and inclusion (EDI) officer;
- intellectual property (IP) manager; and,
- business development and partnerships manager.

Committees

In addition to the Board of directors, executive and operational staff, the proposed network will be expected to establish relevant committees to advance the activities of the network. At a minimum, the lead recipient must put in place a committee for project selection (see section 2.3 Eligible activities for further details).

Conflict of interest framework

Achieving the objectives of the Cyber Security Innovation Network involves various types of interactions among network participants, some of which may place individuals in positions of potential, apparent, or actual conflict of interest. The lead recipient must develop a conflict of interest framework for directors, officers, employees, and committee members to prevent real or perceived conflicts of interest. The framework must include a process for disclosure and a mechanism for conflict management.

Network membership structure

The Cyber Security Innovation Network must put in place a membership structure to formalize the participation of the ecosystem members (other than ultimate recipients who will enter funding agreements with the lead recipient), and provide details on how participants will benefit from the network's activities. The membership structure must clarify the terms under which members join (including payment for membership, if any). Membership may evolve over time, and the proposed participation model must be designed in an inclusive way to ensure all willing participants can join the network and benefit from its activities. Final membership structure will be set out in the contribution agreement.

2.3 Eligible activities

The Cyber Security Innovation Network is expected to undertake activities to enhance research and development, increase commercialization, and develop a pipeline of skilled talent. R&D and commercialization activities can cover Technological Readiness Levels (TRLs) 1 to 9 and could include (Refer to Annex A – Technology readiness level scale for more details):

Collaborative cyber security technology research and development, such as:

- conceptual design, proof-of-concept validation, prototype development, creation of intellectual property, technology/product testing, knowledge mobilization activities; and,
- development of new products, services and/or processes.

Commercialization of innovative cyber security products and services, such as:

- activities related to the exploitation and retention of intellectual property; and,
- business development services for firms to facilitate access to new customers and expand markets, which may include market studies and advisory services, in addition to other business services (e.g., linking start-ups with strategic partners, “pitch days”, marketing activities, etc.)

Development of innovative national approaches to address skills and labour gaps in Canada and to enable Canadian companies to address cyber security challenges, such as:

- identifying and communicating industry-oriented skills needs (e.g., assessment of industry’s current or anticipated workforce needs, building awareness of industry demand for skilled talent across stakeholder groups, environmental scans, workshops, etc.);
- training modules (including upskilling and reskilling solutions);
- development and promotion of education pathways for defined studies in cyber security; curriculum development, and support for teaching capacity to deliver the curriculum;
- coaching/mentoring; and,
- co-op programs and/or other types of Work-Integrated Learning (WIL) opportunities (e.g., apprenticeships, internships, practicums, etc.) and solutions to help businesses onboard students into occupations.

Activities listed above could be undertaken by ultimate recipients and should involve a high degree of collaboration to enhance linkages between partners.

The lead recipient will be responsible for activities related to coordination, oversight, and accountability of network activities in all three areas. These activities could include:

- organization of networking events (such events do not include meetings of a general nature and that are a part of recurring operational requirements);
- organization of conferences and workshops in support of collaborative R&D activities;
- operation of network offices (headquarters and regional offices);
- selection and management of projects; and,
- other activities may be considered eligible and are subject to approval by the Cyber Security Innovation Network program.

Planned and ready projects

To ensure timely implementation of network activities, applicants must provide details in their application about activities already identified and that can be implemented within the first year of network operations, including confirmed cost match.

Network project selection criteria and process

A lead recipient may issue periodic calls for proposals for projects that pertain to the targeted activities outlined above. A lead recipient must implement an assessment framework for the selection and approval of projects. Applicants must provide details about their plans, including timelines and criteria for the selection of network projects. These details will be included in the contribution agreement.

Project selection must be conducted through open, fair, transparent, and expert-driven processes to ensure they meet the standards of merit-based reviews and provide a meaningful contribution to the ecosystem according to the goals of the network.

Project selection criteria will include, at a minimum:

- funding commitment;
- timelines of project delivery;
- assessments of the potential economic, innovation and public benefits;
- technical feasibility of a project;
- areas of cyber security specialization;
- potential for commercialization in Canada (including intellectual property);
- private sector and other partner participation must be representative of the diverse mix of organizations within the cyber security ecosystem in Canada;
- opportunities for collaboration and synergies between projects;
- regional representation;
- financial capacity of ultimate recipients to carry out projects;
- projects contribute to the objectives of the network to enhance R&D, increase commercialization, and develop a pipeline of skilled cyber security talent; and,
- project benefits strengthen and promote the sustainability of the network.

The lead recipient must form a committee responsible for project selection that must meet the following criteria:

- be comprised of one-third (1/3) independent members;
  - independent members are defined as individuals who will not benefit directly from the activities of the organization, and who have no material relationship with the network (and the lead recipient) that could either directly or indirectly, in practice or appearance, impair their ability to think and act in an independent manner that is in the best interests of the network.
- be representative of the cyber security industry, research, and skills ecosystem;
- be pan-Canadian; and,
- respect the principles of equity, diversity, and inclusion.

2.3.1 Eligible costs

The program contribution to any eligible recipient will not exceed 50 percent of its total eligible costs, except for eligible recipients that are academic institutions, where the contribution provided may cover 100 percent of their eligible costs.

Administration and operating costs

Eligible administration and operating costs include costs incurred by the lead recipient that support the day-to-day operations of the network to support its mandate.

Project costs

Eligible project costs relate to the activities undertaken by ultimate recipients to execute the activities of the Cyber Security Innovation Network. Such expenses could include:

a) recruiting and retaining faculty, graduate students, postdoctoral candidates, researchers, support engineers; and, administrative staff;
b) direct costs of research, such as facility access and equipment, material and supplies, salaries, and stipends;
c) costs related to knowledge mobilization, technology exchange and exploitation (e.g., prototype development, market studies, intellectual property related to the centres' research, and policy development); and,
d) up to 20 percent of funds may be used for equipment and infrastructure for research, development, and student/researcher training.

Eligible costs for activities undertaken by the lead and ultimate recipients may be categorized as follows:

a) Direct labour;
b) Subcontractor and consultants;
c) Equipment;
d) Direct costs;
e) Travel and outreach costs; and,
f) Indirect costs (overhead).

Indirect costs (overhead) thresholds of 55 percent on total eligible direct labour and no more than 15 percent of total eligible costs will apply for each lead and ultimate recipients.

Costs occurring outside of Canada cannot represent more than 10 percent of submitted total eligible costs.

On a case-by-case basis, the Minister may consider supporting retroactive reimbursement of eligible costs a lead recipient incurred prior to the signing of the contribution agreement but not earlier than the date on which an application received notice of approval. Retroactively eligible costs shall not exceed 20 percent of total eligible costs. The Minister will not be obliged to pay incurred costs in the event an application is rejected or not approved for funding.

2.3.2 Ineligible costs

Certain costs are not eligible for reimbursement, regardless of whether they are responsibly and properly incurred by a recipient in the performance of the project.

Ineligible costs will include:

a) direct support for professional certification;
b) any form of interest paid or payable on invested capital, bonds, debentures, bank or other loans together with related bond discounts and finance charges; the interest portion of the lease cost that is attributable to cost of borrowing regardless of types of lease;
c) legal, accounting and consulting fees in connection with financial reorganization (including the set-up of new not-for-profit organizations), security issues, capital stock issues, obtaining of licenses, establishment and management of agreements with ultimate recipients, and prosecution of claims against the Minister. Such costs may be eligible if they are in connection with obtaining patents or other statutory protection for project intellectual property;
d) losses on investments, bad debts and expenses for the collection charges;
e) losses on other projects or contracts;
f) federal and provincial income taxes, goods and services taxes, excess profit taxes or surtaxes and/or special expenses in connection with those taxes, except duty taxes paid for importing is eligible cost;
g) provisions for contingencies;
h) premiums for life insurance on the lives of officers and/or directors where proceeds accrue to the lead and/or ultimate recipients;
i) amortization of unrealized appreciation of assets;
j) depreciation of assets paid for by the Minister;
k) fines and penalties;
l) unreasonable compensation for officers and employees;
m) product development or improvement expenses not associated with the work being performed under the project;
n) advertising, except reasonable advertising of an industrial or institutional character placed in trade, technical or professional journals for the dissemination of information for the industry or institution;
o) entertainment expenses including but not limited to, catering, alcohol, non-travel expenses;

p) donations;
q) dues and other memberships other than regular trade and professional associations;
r) extraordinary or abnormal fees for professional advice in regard to technical, administrative or accounting matters, unless approval from the Minister is obtained;
s) selling and marketing expenses associated with the products or services or both being developed under the contribution agreement; and,
t) in-kind costs. In-kind costs are ineligible for reimbursements under the federal contribution but can be provided to meet the cost-matching requirements of the program. Refer to section 2.9 Matching fund requirements for details on cost-matching requirements.

2.4 Cyber security plan

The lead recipient must provide ISED with a cyber security plan for approval before inclusion in the contribution agreement. As part of the application process, applicants must demonstrate how they intend to ensure cyber resilience and strategies to identify, protect, detect, respond and recover from potential cyber security incidents.

The lead recipient must:

- identify cyber risks and vulnerabilities associated with network operations and activities;
- demonstrate how it will strive to implement the path to enterprise security developed by the Canadian Centre for Cyber Security (CCCS), starting with the Baseline Cyber Security Controls for Small and Medium Organizations;
- undertake the Canadian Cyber Security Tool (CCST), a virtual self-assessment tool developed by Public Safety (PS), in collaboration with Communications Security Establishment (CSE) and the Canadian Centre for Cyber Security to provide an overview of their organization’s cyber security posture and operational resilience. The results from the self-assessment will help CCCS provide the lead recipient with guidance and tools to develop the cyber security plan that will be included in the contribution agreement;
- assess ultimate recipients’ cyber security plans and capacity to implement the plan before entering into a funding agreement;
- ensure ultimate recipients and their service providers/suppliers reflect the highest standards of security and integrity in their activities and equipment, with strong reputations and track records in Canada; and,
- report periodically and as needed, any network and/or ultimate recipients’ cyber security incidents and response plans.

Ultimate recipients must:

- submit a cyber security plan to the lead recipient for review that includes information about their cyber posture and how it will implement the Baseline Cyber Security Controls for Small and Medium Organizations developed by the Canadian Centre for Cyber Security.

CyberSecure Canada

Ultimate recipients are encouraged to apply for the CyberSecure Canada certification. CyberSecure Canada is a federal cyber certification program that aims to raise the cyber security baseline among SMEs in Canada, increase consumer confidence in the digital economy, promote international standardization and better positions SMEs to compete globally.

This certification requires the implementation of the baseline security controls developed by the Canadian Centre for Cyber Security. The CyberSecure Canada certification mark gives those certified official recognition by the federal government for demonstrating their compliance to the baseline security controls.

Note on the upcoming national standard on cyber security

In December 2019, the Standards Council of Canada (SCC) engaged the CIO Strategy Council to develop a National Standard of Canada for the CyberSecure Canada certification program. The first edition of the new standard will address baseline security controls. Public consultations in support of the standard took place in winter 2021, and publication of the standard is expected before the end of 2021. The standard is intended to be low burden, easily accessible, affordable, effective, national in scope, and sector neutral. Once the national standard is released, the Cyber Security Innovation Network will be expected to integrate it into its activities and operations.

2.5 Data management strategy

The lead recipient must demonstrate how they will implement a data management strategy that will respect the principles of data management and data privacy in the operations and activities of the network. An effective data management strategy will ensure that information can flow easily between network participants to support effective collaboration over the lifecycle of the data.

The lead recipient must to demonstrate how the following components of a data management strategy will be implemented and apply to both its activities and those of ultimate recipients.

The network data management strategy must include at a minimum:

1- Data management practices:

- data governance (e.g., identify roles and responsibilities of lead and ultimate recipients; develop policies, procedures, and guidelines to ensure authorities and accountabilities associated with network data are implemented, including succession plans, as required);
- data ownership (e.g., ensure there is a clear owner of the data that will be collected, produced, and shared);
- data collection (e.g., guidelines on how existing data will be treated and used; the types of data that will be collected, including whether this would include personal information; the

format in which data will be collected; how collected data will be structured to ensure standardization);

- data sharing (e.g., agreements are in place to ensure interoperability and accessibility by authorized parties);
- data integrity (e.g., common structured data formats and data exchange technologies standards and guidelines for the storage, backup and retention of data are in place); and,
- outline any ethical, legal, and commercial constraints network data may be subject to.

2- Data privacy:

- The network is required to be compliant with privacy laws and ensure both lead and ultimate recipients have legal authority to collect, use, or disclose personal information, safeguard personal information, and otherwise give effect to the rights and obligations provided for in application of privacy laws.

2.6 Intellectual property

The lead and ultimate recipients must take appropriate steps to protect the intellectual property resulting from activities supported by the network (network supported IP) to maximize economic and innovation benefits to Canada.

The lead recipient must provide ISED with a network intellectual property strategy for approval. The network IP strategy will be included in the contribution agreement and ultimate recipient funding agreements. The lead and ultimate recipients must act in a manner consistent with the network IP strategy.

The network IP strategy must include, at a minimum:

- a clear policy on intellectual property ownership and access by members;
- clear policies on technology transfer between academia and industry to increase commercialization of research;
- strategies to encourage collaboration among and exploitation by Canadian stakeholders (e.g., approaches to IP licencing and spin off) to the greatest extent possible;
- a plan to help network participants and ultimate recipients to increase their IP knowledge and expertise (e.g., provide IP education/training/resources, patent landscaping, patent prosecution, freedom to operate analysis, identification of internal and external licensing opportunities, etc.);
- a mechanism/plan for resolving conflicts that may arise between network participants; and,
- a plan to help and encourage network participants and ultimate recipients access independent legal advice and IP business advice and expertise (e.g., sharing information about available resources, IP legal clinics, etc.).

Additionally, as part of its obligations, the lead recipient must:

- assess ultimate recipients’ intellectual property strategies and capacity to implement the strategies before entering into a funding agreement; and,
- evaluate anticipated benefits to Canada resulting from network funded IP.

To ensure intellectual property benefits are realized appropriately, the Cyber Security Innovation Network shall pursue activities designed to maximize economic, innovation and public benefits to Canada through the pursuit of R&D and commercialization activities.

The applicant must ensure that ownership of network funded intellectual property will remain in Canada, and that ultimate recipients retain the ability to exploit network funded IP, for the duration of the project and a minimum of five years following project completion. The length of the term may differ on a case-by-case basis to ensure benefits accrue to Canada and will be defined in the contribution agreement between the Government of Canada and the lead recipient. Any change in intellectual property ownership, or the ability to exploit network funded IP, during the term will require ministerial consent, in writing.

The Government of Canada will not have an ownership interest in the IP resulting from activities funded under the Cyber Security Innovation Network program by virtue solely of having provided the funding.

Security considerations

The lead and ultimate recipients must conduct consistent and appropriate due diligence review of potential security risks to research activities to the network and put in place timely measures to appropriately mitigate these risks.

On March 24, 2021, the Government of Canada released a Research Security Policy Statement and asked members of the joint Government of Canada–Universities Working Group to develop specific risk guidelines to integrate national security considerations into the evaluation and funding of research projects and partnerships.

These guidelines will better position researchers, research institutions and government funders to undertake consistent, risk-targeted due diligence of potential risks to research security. The working group will also provide recommendations for complementary tools and measures to ensure researchers and research organizations working with national security partners have the capacity and resources necessary to implement this guidance. The Government of Canada asked that these guidelines be provided for consideration by June 25, 2021.

As the guidelines become available, they will be integrated in the due diligence assessment process undertaken by the Government of Canada in support of this initiative.

As the guidelines are under development, the Government of Canada encourages stakeholders in Canada’s research ecosystem interested in participating in the Cyber Security Innovation Network to work collaboratively to identify and mitigate potential security risks by utilizing existing tools available through the Safeguarding Your Research portal and Safeguarding Science’s workshops.

The Government of Canada reserves the right to:

- review network projects on national security grounds to ensure any national security risks are identified and addressed;
- impose additional intellectual property obligations on ultimate recipients necessary to ensure that national security risks are addressed, as necessary; and,
- implement additional requirements, on a case-by-case basis. This could include, but is not limited to, inspection of equipment (including IT infrastructure) and periodic security briefings, as appropriate.

The Minister reserves the right to decline the participation of any partners on any grounds, to maintain the security and integrity of the network.

Trusted partners

Only trusted partners who reflect the highest standards of security and integrity in their activities, operations and equipment, with strong reputations and track records in Canada, will be eligible to participate in the Cyber Security Innovation Network program.

Principles that define trusted partners of the Cyber Security Innovation Network program include those:

- whose motivations and intentions are both clear and aligned with the goals of the program;
- who pose a low reputational risk, given their track-record of demonstrated respect for the international norms and values of collaboration (i.e., reciprocity, fairness, honesty, etc.);
- who pose no easily discernable conflict of interest/commitment affiliations that would impede the goals of the program; and,
- who uphold the highest ethical and professional standards, including respect for intellectual property rights, sensitive and personal data, ethical standards, and security standards.

2.7 Official languages

The lead recipient shall provide its communications and services to the public in both official languages of Canada in accordance with the spirit and intent of the *Official Languages Act*.

Specifically, the lead recipient shall:

a. make any announcements or documents for ultimate recipients available in the official language of their choice;
b. actively offer its services to ultimate recipients in the official language of their choice;
c. ensure that any communication aimed at the general public or stakeholders is provided in both official languages; and,
d. where a significant demand exists for services from an ultimate recipient to the public in either official language, ensure that the agreements awarding funding to ultimate recipients include a clause requiring the ultimate recipients' communications to the public meet the linguistic demand.

ISED will comply with all applicable requirements stipulated in Canada's *Official Languages Act*, the related regulations, as well as all federal government policies in this regard. ISED's public communications and literature intended for public distribution related to the Cyber Security Innovation Network will be available in both official languages.

2.8 Equity, diversity, and inclusion framework

The lead recipient is expected to develop and implement an equity, diversity, and inclusion framework to demonstrate the actions the network will take to remove barriers to the participation of individuals from underrepresented groups in network governance, operations and activities as defined in *Canada's Employment Equity Act* (women, Indigenous peoples, persons with disabilities and members of visible minorities).

EDI principles are defined as follows in the context of the program:

- **Equity** is defined as the removal of systemic barriers and biases enabling all individuals to have equal opportunity to access and benefit from the program.
    - To achieve this, individuals who participate in the ecosystem must develop a strong understanding of the systemic barriers and biases faced by individuals from underrepresented groups and put in place measures to address these barriers.
- **Diversity** is defined as differences in race, colour, place of origin, religion, immigrant and newcomer status, ethnic origin, ability, sex, sexual orientation, gender identity, gender expression and age.
    - A diversity of perspectives and lived experiences is fundamental to achieving research and innovation excellence.
- **Inclusion** is defined as the practice of ensuring that all individuals are valued and respected for their contributions and are equally supported.
    - Ensuring that members are integrated and supported is fundamental to achieving research and innovation excellence.

At a minimum, the EDI framework must meet the following requirements:

- include objectives, specific actions to be implemented to meet the objectives of the framework, performance metrics, expected outcomes, and data collection methods to represent progress over the funding period;
- the composition of the permanent Board of directors and senior management must strive to meet a gender parity representation target of 50 percent and a 30 percent target for participation from other underrepresented groups (as stated at section 2.2 Governance structure and management of the guide); and,
    - This target represent the aspirational goals of the 50-30 challenge, an initiative between the Government of Canada, business and diversity organizations. The goal of the program is to challenge Canadian organizations to increase the representation and inclusion of diverse groups within their workplace, while highlighting the benefits of giving all Canadians a seat at the table. The challenge allows participating organizations to strive to achieve their 50 – 30 goals in a way that best suits and reflects their needs and acknowledges the variety of sizes and structures of organizations, including those without Boards of directors or senior management teams.

- selection criteria for network-supported projects and members of selection committees must respect the principles of EDI (as stated at section 2.3 Eligible activities of the guide).

2.9 Matching fund requirements

The lead recipient must provide a 1:1 cost-matching of the federal contribution, for a total of an additional $80 million over four years, to be provided in the form of a combination of cash and/or in-kind contributions. The matching contributions will be expected to come from a combination of non-federal government partners (e.g., private sector, provincial/territorial/municipal governments, and others, such as not-for-profit organizations and Canadian post-secondary institutions). This 1:1 leverage of the $80 million federal contribution is expected to result in a total minimum investment of $160 million over four years.

Applicants must demonstrate how they intend to meet the cost-matching requirements of the program and include, at a minimum, the full cost-matching requirements for the first 12 months of operations at the time of application. Financial and/or in-kind contributions from partners to match the requested funds must be in the form of letters of commitment to be included in the application package. The full terms of cost-matching requirements will be finalized in the contribution agreement.

In-kind contributions

In-kind contributions are defined as cash-equivalent goods or services that replace an incremental expense that would have to be paid with the federal contribution if not provided by other partners. In-kind contributions must be provided at fair market value and be relevant and central to the activities and objectives of the contribution agreement. Examples of in-kind contribution could include equipment (donated and/or loaned); incremental costs associated with access to databases; materials; software; academic researcher salaries, etc. In-kind contributions are ineligible costs under the federal contribution of the Cyber Security Innovation Network program.

Limits on in-kind and cash contributions

The table below outlines the limits of cash and in-kind contributions allowed under the Cyber Security Innovation Network program.

	Year 1 (2021-22)	**Year 2 (2022-23)**	**Year 3 (2023-24)**	**Year 4 (2024-25)**
In-kind	Up to 50 percent	Up to 50 percent	Up to 25 percent	Up to 25 percent
Cash	Up to 50 percent	Up to 50 percent	Up to 75 percent	Up to 75 percent

Funding breakdown

Cyber Security Innovation Network federal contribution (Total of $80 million over four years)	**Matching contributions from combination of private sector, Canadian post-secondary institutions, provincial/territorial/municipal governments, and not-for-profit organizations** (Total of $80 million over four years)
• Cyber Security Innovation Network supports funded eligible costs • Funded eligible costs include administration, operating and project costs • In-kind contributions are ineligible costs	• Matching supports funded eligible costs and/or unfunded eligible costs • Funding toward ineligible costs will not count toward the mandatory 1:1 match

Other funding

Applicants are encouraged to secure cash and/or in-kind contributions over and above the minimum mandatory cost-matching. However, these additional contributions cannot be used to displace the required contribution and will not be matched by the Cyber Security Innovation Network federal contribution. Contributions received from other sources, or contributions that exceed the matching requirement for the maximum federal contribution, can be applied at the discretion of the lead and ultimate recipients, including to activities or costs ineligible under this program. Applicants are required to disclose any support received through other programs that will be used in supporting the network and its activities.

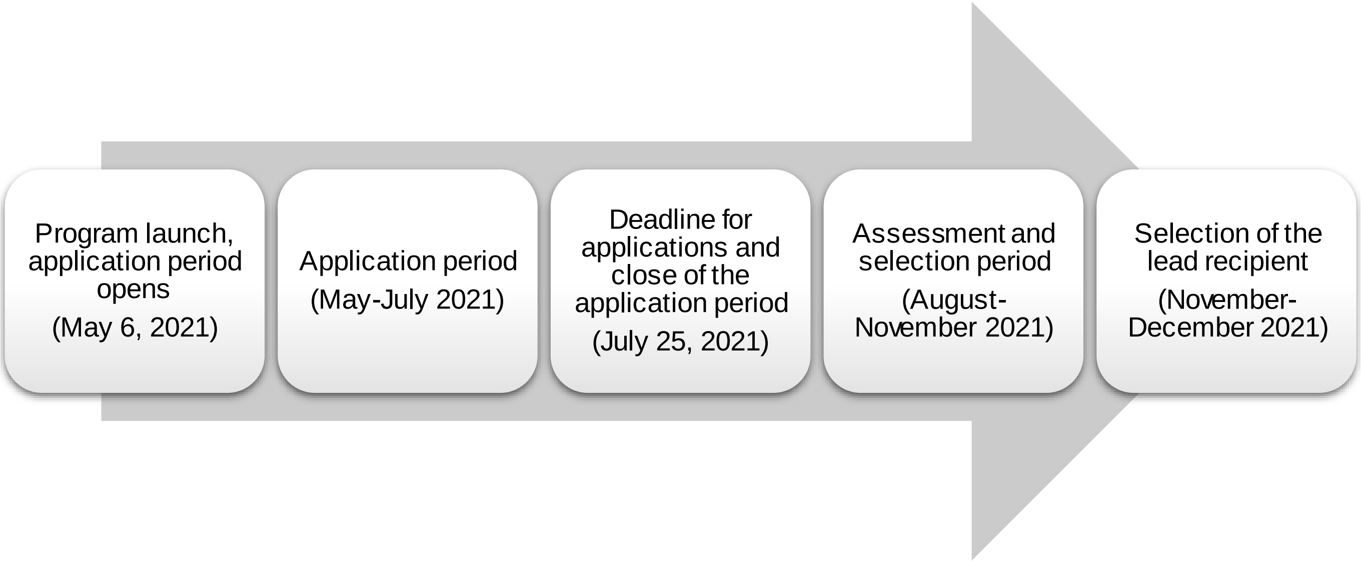
Funding from foreign entities cannot count towards cash or in-kind contributions to the network. Any physical space, activities and equipment used to undertake activities funded by foreign governments must be kept separate from the physical space, equipment and activities of the network.

2.10 Network sustainability plan

The lead recipient is expected to develop a sustainability plan which lays out the strategy to become financially viable and operate the network beyond the federal funding period.

3. Application process

Applicants wishing to apply for the Cyber Security Innovation Network must complete the application package by the submission deadline to be considered. The application and assessment process is anticipated to go ahead as follows:



Program launch, application period opens (May 6, 2021)

Application period (May-July 2021)

Deadline for applications and close of the application period (July 25, 2021)

Assessment and selection period (August-November 2021)

Selection of the lead recipient (November-December 2021)

Figure 1: Visual representation of the Cyber Security Innovation Network application and assessment process. Timelines are subject to change.

3.1 Submission process

Lead applicant

For the purpose of submitting an application to the Cyber Security Innovation Network program, proposed network applicants must be represented by a lead applicant. The lead applicant will be responsible for submitting the application and will be the main point of contact for ISED during the administration of the application process. The lead applicant may be the not-for-profit organization proposed to manage the federal contribution under the Cyber Security Innovation Network program, or a participant taking a leading role in the application process on behalf of its partners. Municipal, provincial, territorial, and federal governments are not eligible to be a lead applicant, nor are individuals.

Applicants are encouraged to read the program guide when preparing an application package.

How to request the application package

To request the Cyber Security Innovation Network application package, please send us an email at: cybersecuritynetwork-reseaucybersecurite@canada.ca

The application package will include the following documentation:

- Application form (MS Word document)
- Appendix A: Financial history of activities supporting cyber security research and development, commercialization, and skills and talent development (for the applicant and centres of expertise on cyber security affiliated with post-secondary institutions) (MS Excel document)
- Appendix B – List of Cyber Security Innovation Network participating organizations (MS Excel document)
- Appendix C – Costing and financing workbook (MS Excel Document)
    - Reference document - Appendix D – Cyber Security Innovation Network cost principles (PDF document)

The Cyber Security Innovation Network application package must be submitted by email at the following address: cybersecuritynetwork-reseaucybersecurite@canada.ca **by 11:59pm Pacific Standard Time (PST) on Sunday, July 25, 2021.** Mailed or facsimile (fax) submissions will not be accepted. Late submissions will not be accepted.

Applicants will receive acknowledgement of the submission of their application within 48 business hours.

The information provided in the application package will be used to complete the assessment and selection process. Completed applications will not be reviewed prior to the close of the application period. Applications that are incomplete or deemed by ISED to not meet the minimum eligibility requirements of the program will not proceed to assessment and applicants will be notified in writing.

4. Assessment and selection process

The selected applicant will be chosen through a transparent, merit-based process to ensure they can meet the objectives and expected outcomes of the contribution program.

4.1 Assessment process

Applications for funding under the Cyber Security Innovation Network will be evaluated in three steps as outlined below.

4.1.1 Step 1 – Initial screening

Following the close of the application period, applications will be reviewed by the Cyber Security Innovation Network program officers to:

- Confirm completeness of applications; and,
- Confirm the eligibility of applicants and proposed activities;

Applicants will be notified in writing as to whether their proposals are moving forward to the full assessment process or are rejected.

4.1.2 Step 2 – Full assessment

ISED will form an advisory group to support the assessment and selection process. The advisory group will consist of subject-matter experts from across the Government of Canada, who will provide relevant expertise and knowledge to assessing the merit, potential and feasibility of an application. Applications will be assessed against the following four categories of criteria:

1. Proposed activities against the three pillars of network activities:

- Research and development;
- Commercialization; and,
- Skills and talent development.

2. Program requirements outlined in section 2 of the program guide, including:

- Intellectual property strategy;
- Data management strategy;
- Cyber security plan;
- Cost-matching requirements;
- Equity, diversity, and inclusion framework; and,
- Network sustainability.

3. Expected benefits to Canada

Innovation benefits

The innovation benefits assessment will examine the following factors:

- ecosystem impact (e.g., network participants are representative of Canada's regions; network participants represent a diversity of organizations across the cyber security ecosystem including SMEs, large enterprises, Canadian post-secondary institutions; and, network complements activities of other stakeholders, including not-for-profit organizations and provincial/territorial/municipal governments);
- level of collaboration (e.g., including leveraged R&D funding and/or in-kind resources by the network for collaborative projects; networking activities proposed to promote collaboration, etc.);
- level of innovation (e.g., incremental to existing products/services vs. new approaches and activities);
- technological advancement (e.g., creation and commercialization of new intellectual property in Canada); and,
- spillover benefits (e.g., creation of key industrial capabilities and strengths; and, benefits to the greater supply chain, industry and/or partners, and a diversity of stakeholders).

Economic benefits

The economic benefits assessment will examine the following factors:

- ability to demonstrate degree of potential disruptive market impact and market advantage of technologies developed through the network (competitiveness);

- clear path to commercialization of network-supported projects; and,
- number of cybersecurity jobs created as a result of network activities and initiatives.

Public benefits

The public benefits assessment will examine the following factors:

- ability to demonstrate the growth of a pipeline of skilled talent (e.g., industry-focused skills needs assessment, skills/training plan in place, including opportunities for training, reskilling/upskilling, co-op and other types of Work-Integrated Learning placements, diversification of talent pipeline) that can address the targeted needs of industry and academia; and,
- the enhancement of under-represented groups, in particular women, in network activities.

Additional benefits

- Applicants are encouraged to provide any additional benefits their proposals may generate that are not articulated above.

4. Due diligence risk assessment

The purpose is to evaluate applicants' capacity to achieve the program's stated objectives. Risks taken into consideration include:

- Managerial and governance;
- Technical and workforce capability;
- Security;
- Financial;
- Trade; and,
- Market.

In addition to assessing proposal(s) against the above set of criteria, the advisory group may be called upon to provide advice on potential areas of collaboration over and above what is provided in an application.

During the full assessment process, ISED may invite applicant(s) to virtual meeting(s) with the advisory group to further discuss proposal(s).

4.1.3 Step 3 – Funding decision

The advisory group will be responsible for reviewing assessment results and provide a consensus-based recommendation to ISED. The Minister of Innovation, Science and Industry will exercise their discretion as to which application(s) to fund.

Selected applicant(s) will be informed of the final decision in fall 2021 in a formal letter from the Minister of ISED. Funding decisions made by ISED are final. There is no appeal process.

4.2 Contribution agreement

Following selection, a contribution agreement between the selected applicant and ISED will be negotiated, signed and executed, and will include the legally binding responsibilities and obligations of both parties. Certain elements of the selected application may be modified during the negotiation of the contribution agreement.

The value of the contribution agreement with the lead recipient will be up to $80 million over four years (2021-22 to 2024-25). Funding will begin according to the date negotiated in the contribution agreement. A contribution agreement will set out obligations to allow the network enough flexibility to respond to changing dynamics in the innovation ecosystem and in the market over the course of the agreement.

The Minister of Innovation, Science and Industry will approve the initial allocation of funding for eligible activities based on the lead recipient's application and subsequent annual corporate plans, which will include its annual cash flow requirements (see section 5. Oversight and monitoring for further details).

4.3 Stacking provisions

Applicants must inform the Minister of any other government (federal, provincial, territorial, municipal) financial assistance it has received or requested.

The combined level of financial assistance from all government sources (federal, provincial, territorial, municipal) to any one eligible recipient shall not exceed 75 percent of eligible costs, except for eligible recipients that are academic institutions from whom the maximum assistance would be 100 percent.

The combined level of assistance provided to the network from all government sources will not exceed 100 percent of the total eligible costs of the network.

4.4 Method of payment

Payments to the lead recipient will be made on the basis of documented claims for actual eligible costs incurred. Claims are to be submitted by the ultimate recipients either individually or combined and presented to ISED by the lead recipient. Each claim is to be accompanied by a brief report of the work completed and details of all costs being claimed and shall be substantiated by such documents that are satisfactory to the Minister. Claims shall be certified by an officer of the lead recipient or by such other person that is satisfactory to the Minister.

The network may be provided advance payments in accordance to an assessment of the risk level, and the network’s forecasted annual cash flow requirements as provided to the Minister by the network. For each fiscal year, the network will provide evidence satisfactory to the Minister of all eligible costs that have been incurred and paid.

4.5 Repayment conditions

Contributions made under the Cyber Security Innovation Network are non-repayable.

5. Oversight and monitoring

5.1 Corporate plans and annual reports

The signed contribution agreement will include the provision that the lead recipient will submit periodic progress reports, claims reports, and annual consolidated financial statements. This information will be used to monitor the performance of the network against the contribution agreement. The lead recipient must provide this information in an annual corporate plan and an annual report.

5.1.1 Corporate plan

The lead recipient shall provide a corporate plan annually to the Minister before January 31 of each year of operation. The corporate plan shall include:

a. reference to the lead recipient’s corporate plan of the current fiscal year (if applicable), including its successes and remaining challenges;
b. planned objectives and activities for the upcoming fiscal year, along with a proposed schedule for their implementation;
c. planned expenditures for the upcoming fiscal year;
d. risk assessment and mitigation strategies;
e. ongoing performance monitoring strategies; and,
f. annual cash flow requirements, including plans to meet 1:1 cost-matching requirement, in respect to eligible costs for the upcoming fiscal year, including funding to be disbursed to ultimate recipients for eligible projects.

5.1.2 Annual report

The lead recipient shall provide an annual report to the Minister, in both official languages of Canada, no later than July 31 of each year of operation. The annual report shall include:

a. reporting on key performance indicators, project benefits to Canada, and results achieved for the previous fiscal year;
b. audited financial statements for the previous fiscal year, prepared in accordance with generally accepted accounting principles and approved by its Board;
c. a statement of the total funding received by the lead recipient from all sources in the previous fiscal year, including all Canadian government assistance, to support eligible activities;
d. a statement of the amount of the contribution directed towards eligible costs in the previous fiscal year, detailed by category of eligible activities;
e. amount of funding leveraged from other sources (if applicable) in the previous fiscal year to support eligible activities;

f. a statement of objectives for the previous fiscal year, as set out in the relevant corporate plan, and a statement on the extent to which the lead recipient met those objectives and any course corrections or deviations from the original objectives that occurred;
g. a statement of objectives for the current fiscal year and for the foreseeable future; and,
h. criteria that were applied to select the eligible activities of ultimate recipients.

Communications

The lead recipient's activities and results should be conveyed to external audiences. Communications are subject to official language requirements (see section 2.7 Official languages for further details). For the duration of the contribution agreement, the lead recipient's communications activities and messages must acknowledge the contribution of the federal government in supporting its activities through the Cyber Security Innovation Network program, in conjunction with the Canada wordmark.

5.2 Monitoring, guidance, and support

Ongoing administration of the program will be provided by ISED officials. ISED officials will work with the lead applicant during the negotiation of the contribution agreement, followed by ongoing oversight and monitoring once the contribution agreement is signed. As part of its administration, ISED will liaise with the lead recipient, which may include periodic observer attendance at Board of Directors meetings, meetings and/or visits to ensure the implementation of the contribution agreement is on track.

Regular and frequent contact will facilitate the sharing of information between both parties to the contribution agreement. ISED's administration will permit the collection of information to guide federal policy and program directions, and the facilitation of linkages between the lead recipient and other federal organizations, as applicable.

5.3 Expected outcomes and performance indicators

The lead recipient will collect qualitative and quantitative performance information from ultimate recipients to measure progress towards meeting the network's expected outcomes and ability to generate results from its proposed activities. Below is a chart listing expected outcomes and performance indicators that must be reported on by the lead recipient. Expected outcomes and performance indicators may be adjusted during the negotiations of the contribution agreement and targets will be negotiated at that time to reflect the selected network proposal.

Short-Term outcomes (2021-2022 to 2022-23)	
Outcomes	**Performance indicators**
Ecosystem impact	
National scope	Number of Provinces/Territories represented in the network
Comprehensive inclusion of diverse stakeholders from across the country	Number of network participants from across academia, private sector, not-for-profit organizations, etc. by type and geographic location

Research and Development	
Ecosystem collaboration	Dollar and/or in-kind value leveraged by the network from private sector and/or other partners
Skills and talent development	
Increased resources (people and tools) available to identify, design, and deliver skills and talent development solutions	Common curriculum framework developed by the network informed by a shared understanding of industry skills needs
	Number of new cyber security instructors/trainers, including industry leaders and practitioners recruited in post-secondary institutions as a result of network activities
Medium-Term outcomes (2023-24 to 2024-25)	
Outcomes	**Performance indicators**
Research and Development	
Increased collaboration between industry and academia	Number of collaborative R&D projects that involve both industry and academic participants
Commercialization	
Network projects advance product and knowledge development towards commercialization	Number of projects that advance over a minimum of two Technological Readiness Levels (TRLs)
	Number of patents filed and/or granted as a result of network activities
Skills and talent development	
Increased opportunities for students and cyber security workers to develop cyber security related skills and knowledge	Number of new post-secondary students participating in cyber security training activities (courses, programs, etc.)
	Number of participants from underrepresented groups, including women, engaged in cyber security skills development activities through the network
	Number of workers in cyber-related fields participating in cyber security training, reskilling and upskilling activities established by the network
	Number of post-secondary students participating in co-op and/or Work-Integrated Learning programs established by the network

Long-Term outcomes (2025-26 to 2026-27 and onwards)	
Outcomes	**Performance indicators**
Commercialization	
Canadian businesses commercialize new or improved cyber security innovations	Value of sales of cyber security products and services
Skills and talent development	
Industry can access qualified and skilled cyber security pipeline	Number of people holding credentials in cyber security
	Number of graduates of academic programs and trainees entering the cyber security workforce
	Percentage of cyber security professionals from underrepresented groups, including women, entering the workforce
	Percentage of firms participating in the network indicating recent graduates of academic programs and trainees entering the workforce meet industry needs

6. Policies and considerations

6.1 *Access to Information Act* and the *Privacy Act*

The Cyber Security Innovation Network is subject to the federal *Access to Information Act* and the *Privacy Act*.

6.2 Security of organization information

ISED will not disclose to any party outside of the federal government (other than parties retained to review technical aspects of an application) any commercially confidential information an applicant submits, except in the following circumstances:

- The company authorizes the release;
- ISED is required by law to release the information;
- The information ceases to be confidential; and,
- The Minister of ISED is required to release the information to an international or internal trade panel due to a dispute in which Canada is a party or a third-party intervener.

Applicants must mark any commercially confidential information in their application as such. Applicants may also wish to become familiar with the terms of the *Access to Information Act*, which governs the release of information held by federal organizations.

An electronic copy of all applications, regardless of the results of the assessment process, will be retained for ten (10) years for record keeping purposes. After ten (10) years it will be destroyed. Applications received outside the application period will be returned to the applicant directly, unread, and unassessed.

6.3 *Lobbying Act* and *Conflict of Interest Act*

As part of the application process, applicants are required to provide the following:

- An affirmation that any person, including any consultant or in-house lobbyist who lobbies on its behalf to obtain funding under the Cyber Security Innovation Network, and who is required to be registered pursuant to the *Lobbying Act*, is registered pursuant to the Act. For more information on lobbying and the *Lobbying Act*, consult the Office of the Commissioner of Lobbying of Canada;
- An affirmation that the applicant has not, and neither has any person on its behalf, engaged or employed any person (other than an employee) for the purposes of obtaining funding from the Cyber Security Innovation Network; and paid, or agreed to pay that person, a commission, contingency or success fee or any other consideration (whether monetary or otherwise) that is dependent upon the applicant receiving program funding;
- Assurance that any former public servant, who derives benefit from the contribution agreement, will be in compliance with the *Values and Ethics Code for the Public Sector*, the *Policy on People Management*, and the *Directive on Conflict of Interest*;
- Assurance that any former public officer holder, who derives benefit from the contribution agreement, will be in compliance with the *Conflict of Interest Act*;
- Assurance that no member of the House of Commons or Senate will benefit from the contribution agreement; and,
- An attestation from key executives indicating that any contributions from the program is not included in the evaluation of, nor be used for, executive performance pay.

6.4 International agreements

The Cyber Security Innovation Network is administered according to Canada's international agreements. Contributions are not contingent, in law or in fact, on actual or anticipated export performance.

7. Other information

7.1 Public website

ISED's website provides information regarding program objectives, requirements and how to apply to the Cyber Security Innovation Network program.

7.2 Contact us

Email
The Cyber Security Innovation Network program team can be reached at: cybersecuritynetwork-reseaucybersecurite@canada.ca

Phone
ISED Citizen Services Centre
Telephone (toll-free in Canada): 1-800-328-6189
Telephone (international): 613-954-5031
TTY (for hearing impaired): 1-866-694-8389
Business hours: 8:30 a.m. to 5:00 p.m. (Eastern Time)

Mailing address
Cyber Security Innovation Network
C.D. Howe Building
235 Queen Street, 9th floor, East Tower
Ottawa, ON K1A 0H5
Canada

Definitions

Applicant	Comprised as a network of three or more Canadian centres of expertise on cyber security affiliated with post-secondary institutions, private sector partners and others, incorporated as a not-for-profit organization under the *Canada Not-for-Profit Corporations Act.*
Application	Refers to the completed application form and supporting documents submitted to ISED to be considered under the Cyber Security Innovation Network program.
Center of expertise on cyber security affiliated with a post-secondary institution	Defined as an organization affiliated with a recognized Canadian post-secondary institution that support the growth of the cyber security innovation ecosystem.
Conflict of interest	Means a situation where, to the detriment or potential detriment to the Cyber Security Innovation Network, an individual participating in the network is, or may be, in a position to use research knowledge, authority or influence for personal or family gain (financial or other) or to benefit others.
Contribution agreement	A written agreement between the Government of Canada and the selected applicant that sets out the obligations or understandings of both with respect to the transfer payment. Upon execution of a contribution agreement, the selected applicant is referred to as the lead recipient. The Government of Canada is responsible for drafting the program contribution agreement to be negotiated with the selected applicant.
Cyber security	The protection of digital information and the infrastructure on which it resides.
Due diligence	A method of assessing applications, which will examine the ability of applicants to implement and achieve the stated objectives outlined in the application.

Eligible activities	Activities that are eligible for funding under the Cyber Security Innovation Network program.
Eligible costs	The costs to which the Cyber Security Innovation Network program makes a financial contribution (to cover the whole cost, or part of the cost) as established by the contribution agreement with the lead recipient.
Expected benefits	The economic, innovation, public and other benefits that are expected to result from the network's activities.
Fiscal year	As per the *Financial Administration Act (*FAA) a fiscal year is defined as the period beginning on April 1 in one year and ending on March 31 in the next year.
Ineligible costs	Costs that are not eligible for reimbursement under the Cyber Security Innovation Network program.
In-kind contribution	In-kind contributions may include the fair market value of a non-cash contribution provided to the project in the form of goods, and/or services provided by a partner. Fair market value means the price that would be agreed to in an open and unrestricted market between knowledgeable and willing parties dealing at arm's length, who are fully informed and not under any compulsion to transact.
Innovation, Science and Economic Development Canada (ISED)	Innovation, Science and Economic Development Canada is the federal department responsible for administering the Cyber Security Innovation Network program.
Lead applicant	ISED's main point of contact during the administration of the application process. The lead applicant may be the not-for-profit organization proposed to manage the federal contribution under the Cyber Security Innovation Network program, or a participant making up the network and taking a leading role in the application process. Municipal, provincial, territorial, and federal governments are not eligible to be a lead applicant, nor are individuals.

Letter of commitment	Demonstrate the network has secured cash and/or in-kind contributions committed by partners contributing towards the cost-matching requirement of the Cyber Security Innovation Network program. Letters of commitment must be signed by a senior executive with signing authority for the contribution (C-level executive), and provided on official letterhead.
Participating organizations (also referred to as network participants)	Participating organizations are those that will play a role in the applicant's proposal. Types of participating organizations may include: ○ centres of expertise on cyber security affiliated with post-secondary institutions (other than the centres coming forward as applicants); ○ private sector (including both small and medium sized enterprises and larger enterprises); ○ Canadian post-secondary institutions (e.g., research centres, universities, colleges, polytechnics); ○ not-for-profit organizations (e.g., industry associations, incubators and accelerators, skills development organizations, etc.); and, ○ provincial/territorial/municipal governments. Participating organizations may: • contribute to the cost-matching requirement of the program and carry-out project activities; • carry-out project activities and not contribute to the cost-matching requirements (e.g., ultimate recipients could be selected as a result of a call for proposals and receive network funding only); • contribute to the cost-matching requirements only (e.g., contribute funding to the network and not carry-out project activities); and, • join the network in another capacity (to be defined by the applicant).

Partner	The following categories of partners are expected to be included in the network proposal (but are not limited to): • centres of expertise on cyber security affiliated with post-secondary institutions (other than the centres coming forward as applicants); • private sector (including both small and medium sized enterprises and larger enterprises); • Canadian post-secondary institutions (e.g., research centres, universities, colleges, polytechnics); • not-for-profit organizations (e.g., industry associations, incubators and accelerators, skills development organizations, etc.); and, • provincial/territorial/municipal governments.
Project	The collective activities that are undertaken to accomplish the Cyber Security Innovation Network's program objectives under the three pillar of network activities (research and development; commercialization and skills and talent development).

Annex A – Technology readiness level scale

Technology Readiness Level	Description
TRL 1—Basic principles of concept are observed and reported	Lowest level of technology readiness. Scientific research begins to be translated into applied research and development . Activities might include paper studies of a technology's basic properties.
TRL 2—Technology concept and/or application formulated	Invention begins. Once basic principles are observed, practical applications can be invented. Applications are speculative, and there may be no proof or detailed analysis to support the assumptions. Activities are limited to analytic studies.
TRL 3—Analytical and experimental critical function and/or proof of concept	Active research and development is initiated. This includes analytical studies and/or laboratory studies. Activities might include components that are not yet integrated or representative.
TRL 4—Component and/or validation in laboratory environment	Basic technological components are integrated to establish that they work together. Activities include integration of “ad hoc” hardware in the laboratory.
TRL 5—Component and/or validation in simulated environment	The basic technological components are integrated for testing in a simulated environment. Activities include laboratory integration of components.
TRL 6—System/subsystem model or prototype demonstration in a simulated environment	A model or prototype that represents a near desired configuration. Activities include testing in a simulated operational environment or laboratory. Levels 7 through 9 represent the pre commercialization gap for innovations.
TRL 7—Prototype ready for demonstration in an appropriate operational environment	Prototype at planned operational level and is ready for demonstration in an operational environment. Activities include prototype field testing.
TRL 8—Actual technology completed and qualified through tests and demonstrations	Technology has been proven to work in its final form and under expected conditions. Activities include developmental testing and evaluation of whether it will meet operational requirements.
TRL 9—Actual technology proven through successful deployment in an operational setting	Actual application of the technology in its final form and under real-life conditions, such as those encountered in operational tests and evaluations. Activities include using the innovation under operational conditions.

Innovation, Science and
Economic Development Canada

Innovation, Sciences et
Développement économique Canada

Canada