National Defence Défense nationale

CANADIAN ARMED FORCES

FORCES ARMÉES CANADIENNES

Bureau of Research, Engineering and Advanced Leadership in Innovation and Science (BOREALIS)

From Innovation to Operational Advantage: Defence Innovation Secure Hubs (DISH)

APPLICANT GUIDE

Canada

Summary of Key Information

- Funding mechanism: Non-repayable contribution
- Indicative annual funding profile per DISH (non-binding):
  - **Year 1 (FY 2026–27):** typically, in the range of approximately **$5–10 million**, depending on the scope and scale of proposed establishment and early delivery activities.
  - **Year 2 (FY 2027–28):** typically, in the range of approximately **$10–15 million**, depending on the scope and scale of scaled operations and programmatic activity.
- Duration of contribution: Up to the end of March 2028
- Team composition: **Proposals must include multidisciplinary teams of partners from at least two separate eligible organizations and/or institutions** necessary to deliver the objectives of the proposed DISH
- One eligible Canadian organization must be identified as the **Lead Applicant** and will act as the **Initial Recipient** for the purposes of the contribution agreement

1. Context

Defence Innovation Secure Hubs (DISHs) are secure, mission-oriented hubs established to enable collaboration between government, industry, and academia in support of Canada's defence and national security priorities. DISHs provide trusted environments, infrastructure, and services that support the design, testing, validation, and transition of advanced technologies toward operational use.

DISHs are intended to address a persistent gap in the defence innovation ecosystem: while Canada has strong research and development capacity, innovators often face barriers to engaging with defence organizations, accessing secure environments, and advancing technologies beyond early development. DISHs are designed to support both early engagement and later-stage integration activities, including experimentation, testing, and transition in secure settings. DISHs reduce these barriers by enabling structured, secure, and mission-focused engagement with defence stakeholders.

Each DISH focuses on a defined priority mission area and operates as a stand-alone hub with clear governance and accountability. Collectively, the hubs form a national network that supports the delivery of defence and security capabilities. DISHs are delivered under BOREALIS, the Government of Canada's defence innovation coordination mechanism, which provides strategic coherence, alignment across federal innovation programs, and a single window for engagement on priority defence and security innovation initiatives.

2. The Challenge

Canada's defence and national security organizations are operating in an environment characterized by rapid technological change, increasing system complexity, and heightened security requirements. Two technology areas in particular, **quantum technologies** and **uncrewed systems (UxS),** are expected to have a significant impact on future defence and security operations. While innovation in both domains is advancing rapidly across academia and industry, challenges remain in advancing these technologies into defence and security applications. **Additional context on the quantum and UxS challenge areas is provided in Annex A.**

Quantum

In the quantum domain, Canada has strong research and innovation capabilities spanning sensing, communications, computing, and cryptography. However, transitioning quantum technologies from laboratory demonstrations to defence and security applications presents distinct challenges. These include the need for access to **specialized infrastructure**, **secure environments**, and **defence-relevant use**

cases against which technologies can be tested and validated. Innovators often lack pathways to engage with defence stakeholders early enough to ensure operational relevance, while defence organizations face challenges in assessing maturity, risk, and integration potential in a rapidly evolving and highly specialized field.

As quantum technologies approach thresholds of operational relevance, there is an increasing need for environments that support **secure experimentation, system-level integration, and validation** under conditions that reflect defence and national security constraints. Without such environments, promising technologies risk remaining disconnected from real-world defence needs or advancing in directions misaligned with operational priorities.

Uncrewed and Autonomous Systems (UxS)

In the UxS domain, innovation spans platforms, sensors, communications, autonomy software, and enabling systems. While many UxS technologies demonstrate promise at early stages, advancing them into defence and security contexts requires overcoming challenges related to secure testing, integration with existing systems, interoperability, regulatory compliance, and validation against operational concepts.

Innovators often face limited access to defence users, controlled testing environments, and opportunities to integrate their technologies into broader systems-of-systems. At the same time, defence organizations must assess not only individual components, but how uncrewed and autonomous systems perform when integrated, operated at scale, and deployed in contested or constrained environments.

Secure Environments as a Cross-Cutting Challenge

Across both the quantum and UxS domains, a core barrier is the **lack of access to secure collaboration environments**. Many activities required to advance technologies toward operational relevance, such as integration, system-level testing, and validation with defence users, cannot be conducted in open or unclassified settings.

Defence and national security organizations require environments that can support work at **elevated security levels**, including facilities and digital environments capable of being **accredited up to Level II (Secret)**. Establishing and operating such environments is complex and resource-intensive and is often beyond the capacity of individual innovators or organizations acting alone. The absence of shared, trusted secure environments therefore represents a systemic challenge in transitioning emerging technologies into defence and security applications.

Mission Focus

For the purposes of this Call for Proposals (CFP), **"mission-focused"** refers to activities that are anchored in defence and national security use cases, informed by operational constraints, and aligned with the needs of intended end users. Mission focus goes beyond technology development to consider how capabilities are integrated, tested, validated, and transitioned within real-world defence and security contexts. In the **quantum** domain, mission-oriented activities may include advancing technologies toward defence-relevant applications such as sensing, networking, or computing under security, integration, and operational constraints. In the **UxS** domain, mission-oriented activities may include advancing uncrewed and autonomous systems and enabling technologies through system-level integration, testing, and validation aligned with defence concepts of operation.

Addressing the Challenge through DISH

This CFP seeks to address these challenges by establishing **Defence Innovation Secure Hubs (DISHs)** focused on the **quantum** and **UxS** mission areas. DISHs are intended to provide **secure, mission-oriented environments** where government, industry, and academia can collaborate over time to advance technologies beyond early development and toward defence and security application.

Through access to trusted environments, infrastructure, and sustained engagement with defence stakeholders, DISHs will enable activities such as experimentation, testing, system integration, and validation, supporting clearer pathways from innovation to operational acceptance.

3. Eligibility

This CFP is open to proposals submitted by eligible Canadian organizations, in partnership with other eligible organizations, to establish and operate a DISH.

Eligible **Lead Applicant** organizations or institutions are:

- Canadian incorporated for-profit organizations
- Canadian incorporated not-for-profit organizations
- Canadian universities or other post-secondary institutions chartered in Canada

The Lead Applicant will act as the Recipient for the purposes of the contribution agreement and will assume overall responsibility for the proposed DISH.

Eligible **Partner organizations** or institutions are:

- Canadian universities and other post-secondary institutions chartered in Canada;
- Canadian incorporated for-profit organizations
- Canadian incorporated not-for-profit organizations
- Canadian provincial, territorial and municipal government organizations

All organizations/institutions must possess the legal status necessary to enter into a contribution agreement.

Federal departments, agencies, and crown corporations are not eligible for funding. Furthermore, proposals must not assume or include the use of federally owned infrastructure or facilities, including infrastructure owned or operated by the Department of National Defence or the Canadian Armed Forces, as part of the proposed DISH.

3.1 DISH Team Composition

Each proposal must identify a **Lead Applicant (Initial Recipient)** and one or more **Partner organizations (Ultimate Recipients)** that together form the DISH delivery team.

The **Lead Applicant** is responsible for the overall governance, operation, and management of the DISH and will serve as the primary point of contact with the Department of National Defence (DND) throughout the application process and the contribution funding period. The Lead Applicant must agree to assume administrative and financial responsibility for the DISH.

The Lead Applicant is expected to fulfill the following roles and responsibilities:

- Act as signatory to the Contribution Agreement with DND on behalf of the DISH.
- Ensure that all costs submitted to DND are eligible costs.
- Receive, manage, and distribute contribution funds, where applicable, to Partner organizations in support of eligible activities.
- Establish and manage agreements with Partner organizations, including arrangements related to collaboration, funding flows, and intellectual property, as required.
- Monitor and report to DND on activities and achieved results per the Contribution Agreement requirements.

Partner organizations contribute to the delivery of the DISH by providing expertise, infrastructure, services, or capabilities necessary to achieve the objectives of the proposed hub. Partner organizations may receive funding under this CFP through the Lead Applicant and must enter into appropriate agreements with the Lead Applicant to carry out their roles.

Proposals must include multidisciplinary teams of partners from at least two separate eligible organizations and/or institutions.

3.2 Eligible DISH Activities

Applications must include both:

- **Secure Infrastructure:** a credible and well-justified approach to fitting-up existing facilities, maintaining, and operating secure DISH infrastructure, including a phased plan to achieve accreditation at the appropriate security levels over the funding period, and
- **R&D Plan:** a substantive, coherent program of research and development (R&D) to be delivered through that infrastructure, aligned with one or more of the challenge areas identified in this CFP (quantum and uncrewed systems (UxS)).

Eligible activities may include, but are not limited to:

- Establishment, fit-up, maintenance, and operation of secure physical and/or digital environments, including modifications to existing infrastructure required to enable secure collaborative work at Level II (Secret), as part of a broader hub capability. These activities cannot exceed 50% of total proposed cost, see Annex C for more details. Note: facilities are not required to be accredited to Level II (Secret) at the time of application; proposals must instead demonstrate a credible plan to achieve appropriate security enablement within the funding period.
- Design and delivery of programmatic R&D activities that enable experimentation, testing, system integration, and validation.
- Provision of technical, operational, and coordination services that support collaboration between government, industry, and academia.
- Engagement and facilitation activities that connect innovators with defence and security stakeholders.
- Activities that support the transition and adoption of technologies toward defence and national security application.

Activities related to new construction are not eligible under this CFP.

4. Funding

4.1 Available Funding and Duration

Funding under this Call for Proposals is provided by BOREALIS and delivered through the **Innovation for Defence Excellence and Security (IDEaS) Program** to support the **time-limited establishment and operation of DISHs**.

Funding will be provided in the form of a **non-repayable contribution** through a contribution agreement between the Government of Canada and the successful Lead Applicant.

Contribution Duration

Contribution agreements resulting from this CFP may have a duration of **up to 24 months**, with activities expected to conclude **no later than the end of March 2028**.

Total Funding Envelope

For planning purposes, the Government of Canada anticipates a **total funding envelope of up to $50 million** under this CFP, subject to the receipt of proposals of sufficient quality.

Indicative Annual Funding Profile

For planning purposes only, applicants should note the following **indicative annual funding expectations**, over the maximum contribution agreement duration. **Funding requirements may vary depending on the challenge area, scope, and nature of the proposed DISH.**

Year 1 (FY 2026–27):
Funding supports establishment activities, including secure environment development, initial operations, and early delivery of hub activities. Funding in the range of approximately $5–10 million may be appropriate, depending on the scope and scale of proposed activities. Applicants should request funding that is reasonable and well-justified.

Year 2 (FY 2027–28):
Funding supports scaled operations and increased programmatic activity following establishment of the DISH. Funding in the range of approximately $10–15 million may be appropriate, depending on the scope and scale of proposed activities.

These figures are **indicative and non-binding** and do not represent funding caps or guarantees.

Funding Flexibility

The Government of Canada reserves the right to:

- Fund proposals at levels **below the amounts requested**
- **Adjust funding profiles** across fiscal years
- **Negotiate scope, milestones, and funding levels** prior to finalizing contribution agreements

4.2 Stacking Provisions and Other Government Assistance

The total Canadian government (federal, provincial/territorial and municipal) assistance cannot exceed 100% of total proposal costs. Applicants must identify all sources of funding in their proposals and confirm this information in a Contribution Agreement if the proposal is selected for funding.

4.3 Eligible Costs

Eligible costs are those that are approved and incurred by the Lead Applicant and Partner organizations which, in the opinion of DND, are reasonable and necessary to carry out the eligible DISH activities. Eligible costs will be limited to the actual, non-recurring, and incremental costs of the Lead Applicant and Partner organizations that are directly associated with the establishment and operation of the approved DISH and that are required to achieve the expected results. More details on eligible and ineligible costs are included in Annex C – Eligible and Ineligible Costs.

4.4 Canadian Content

Generally, eligible costs, under all cost categories, are to be incurred in Canada. However, IDEaS may support eligible activities and associated costs incurred outside of Canada when such expenditures are necessary to achieve proposal objectives. In all cases, no more than 50% of eligible costs may be incurred outside of Canada. DISHs must ensure the compliance with this requirement.

4.5 Other Sources of Funding: Cash and In-Kind Contributions

Applicants are encouraged, but not required, to demonstrate relevance, sustainability, and collaboration by leveraging cash and/or in-kind contributions from other sources in support of the proposed Defence Innovation Secure Hub (DISH).

In-kind contributions are cash-equivalent goods or services provided by an organization to the DISH that represent an incremental expense that would otherwise need to be incurred to deliver the proposed hub activities. Examples may include, but are not limited to, access to facilities or infrastructure, data, software, intellectual property, personnel time, or specialized equipment.

Cash contributions may be used to complement IDEaS funding by supporting additional activities, enhancing hub capacity, or expanding the scope of DISH operations beyond what could be achieved through IDEaS funding alone.

Where applicable, cash and in-kind contributions should be clearly described in the proposal, including their source, nature, and intended use. Contributions provided by Partner organizations or third parties are expected to be managed by the Lead Applicant in accordance with appropriate agreements among participating organizations.

5. Proposal form and submission

5.1 Proposal form

Applicants must use the *Defence Innovation Secure Hubs (DISH) Proposal* form. Applicants are and will remain solely responsible for the accuracy and completeness of their submission. Applicants should read the applicant guide and the challenge statement in its entirety prior to submitting their proposal.

The proposal must be submitted by an eligible Lead Applicant/ (see 3.1), by the stated deadline. No proposal submissions will be accepted after the deadline. Proposals not using the DISH proposal form will not be accepted for consideration.

Applicants may submit more than one proposal; however, each proposal must be distinct, self-contained, and free of interdependencies. If proposals are determined to be dependent on one another, they will be deemed inadmissible and will not be considered further.

Individuals from eligible organizations may also participate in more than one DISH. In these cases, all R&D activities must be unique to each DISH and must not rely on or overlap with activities in another DISH.

Recipients involved in multiple selected proposals must submit separate actuals reports for each DISH. Only the eligible costs that are directly tied to achieving the objectives of the specific DISH funded by DND may be included.

Deadline to submit: 2:00 PM (Eastern Time), Thursday, April 2, 2026.

In their proposal, applicants should demonstrate their capability and describe their approach in a thorough, concise and clear manner for carrying out the work. The applicant's responses in the proposal form will be used to develop Schedule A of the Contribution Agreement for the DISH. The proposal should address clearly and in sufficient depth the points that are subject to the evaluation criteria against which the proposal will be evaluated.

To maintain the integrity of the evaluation, evaluators will consider only information presented in the proposal. No information will be inferred, and personal knowledge or beliefs will not be utilized in the evaluation. Applicants should explicitly demonstrate, in sufficient detail, how all criteria are met.

Letters of support, endorsement, or recommendation will not be accepted or considered as part of the proposal. Applicants should not submit letters of support or reference them in their responses. Any such material, if submitted or referenced, will not be considered during the evaluation process.

All costs identified in the proposal must be in Canadian dollars.

It is the applicant's responsibility to ensure that the application and all proposed activities comply with all relevant federal, provincial and territorial legislation and municipal bylaws.

5.2 Proposal submission

Applicants are required to register and submit their proposal(s) using the CPC Connect provided by Canada Post Corporation (CPC). CPC Connect is a digital delivery platform that facilitates sending and receiving confidential messages and documents. Proposals submitted by email will not be accepted. It is the applicant’s responsibility to create an account with CPC Connect and complete all required steps to submit the proposal. Applicants must request their Connect conversation at least five (5) days prior to the CFP closing.

Classified proposals will not be accepted for this CFP.

Submission Process

#	Action	Details
1.	Create a CPC Connect account	**Existing Account:** - If you have an existing account, proceed to Step 2. **New Account Registration:** - Create an account on CPC Connect. - Click on "Login to Connect" on the CPC Connect webpage. - Select "Register now" and complete your personal Canada Post profile. - **Note**: There is no cost to register.

2.	Request a Connect Conversation	**How to Request**: - Send an email to borealisjointprogramoffice-bureaudeprogrammeintegreborealis@forces.gc.ca requesting a Connect conversation. - The email must be sent at least five (5) business days prior to the CFP closing date. - Once requested, the BOREALIS team will initiate the Connect conversation. **Email Notification:** - The applicant will receive an email notification from CPC prompting them to access the conversation. - Through this conversation, the applicant will be able to submit their proposal before the CFP deadline. **Important**: - Each proposal must have a unique title and file number (assigned by BOREALIS team). - When requesting a conversation, indicate the number of proposals to ensure individual file numbers are assigned.
3.	Submit the Proposal via CPC Connect	**Upload Your Proposal**: - Submit the proposal by uploading it within the Connect conversation. - Ensure submission occurs **before the CFP closing date and time**. **Confirmation**: - A confirmation message will be provided within the Connect conversation after submission or after the CFP closes. - Ensure the proposal includes the applicant's full contact information.

5.3 Transmission issues or late submissions

DND will not be responsible for any failure attributable to the transmission or receipt of the proposal including, but not limited to, the following:

- Receipt of a garbled, corrupted, incomplete or illegible proposal;
- Equipment or system incompatibility;
- CPC Connect service disruptions or errors;
- Delays of any kind;
- Inability to establish an electronic conversation, or
- Security of proposal data.

Late submissions will not be accepted.

6. Proposal Evaluation

Proposals will be reviewed according to the criteria listed in Annex B, Evaluation Criteria. Proposals will be reviewed by subject matter experts selected by BOREALIS and may include representatives of other Canadian government departments.

BOREALIS may select one proposal, multiple proposals, or no proposals for funding consideration. At this stage, all applicants will be informed of the status of their proposal after evaluation.

Applicants of selected proposals may be requested to provide additional information to support the final funding selection decisions. Additional proposal analysis may be required, including Financial Risk and Technical Assessments. Failure to submit any information supporting these analyses in a timely fashion may result in elimination from the process.

Before a final decision is made, DND may seek input and advice from other organizations, including, but not limited to, federal, provincial, territorial and municipal government agencies and organizations.

7. Privacy Notice Statement

DND will comply with the federal *Access to Information Act* and *Privacy Act* with respect to proposals received. By submitting personal information, an applicant is consenting to its collection, use and disclosure in accordance with the following Privacy Notice Statement, which explains how the applicant's information will be managed.

Necessary measures have been taken to protect the confidentiality of the information provided by applicants. This information is collected under the authority of the terms and conditions for the IDEaS Transfer Payment Program under DND.

Personal information included in all proposals will be kept along with the proposal results as Information Records of Business Value and retained. This information is protected under the *Access to Information* and *Privacy Act*. According to the *Privacy Act*, data linked to an individual and included in the proposal being evaluated can be accessed by the specific concerned individual who has rights with respect to this information. This individual may, upon request:
(1) be given access to his/her data by making an official privacy request through DND for the attention of the Director, Access to Information and Privacy (DAIP), and
(2) have incorrect information corrected or have a notation attached.

The *Access to Information Act* governs the protection and disclosure of information, confidential or otherwise, supplied to a federal government institution.

Paragraph 20(1) (b) of the Act states that:

> a government institution [such as DND] shall refuse to disclose any record requested under the Act that contains financial, commercial, scientific or technical information that is confidential information supplied to a government institution by a third party and is treated consistently in a confidential manner by the third party.

Paragraph 20(1) (b) of the Act sets out two mandatory criteria in order to protect applicants' confidential information supplied to DND from disclosure. First, the applicants' documents supplied to DND must contain financial, commercial, scientific or technical information. Second, the applicant must consistently treat such information in a confidential manner. In other words, DND will protect the applicant's confidential information in its possession as much as the applicant protects said confidential information in their own establishment.

Any Privacy or Access to Information request made under their respective Act and completed, will be retained by DAIP for a duration of two (2) years following after the date the request was responded to. After the retention period of two (2) years, the Privacy or Access to Information request file will be destroyed.

For additional information on privacy matters prior to submitting a proposal, please contact:

Director, Access to Information and Privacy (DAIP)
Department of National Defence (DND)
Telephone: direct: 613-992-0996 or toll free: 1-888-272-8207
Email: ATIP-AIPRP@forces.gc.ca

Applicants shall note that key information related to all contribution agreements (e.g., amount, name of the Initial and Ultimate Recipients and location) will be made available to the public on DND's website.

8. Enquiries about the CFP

It is the responsibility of the applicant to obtain clarification of the information contained herein before submitting an application.

Enquiries related to this CFP must be sent to BOREALIS at: borealisjointprogramoffice-bureaudeprogrammeintegreborealis@forces.gc.ca with the subject line "DISH CFP Enquiry", no later than five (5) calendar days before the CFP closing date. Enquiries received after this deadline may not be answered. Applicants must clearly reference as the relevant numbered item of this CFP and provide sufficient detail to enable an accurate response.

Questions and Answers received during the CFP period may be made available to all applicants.

9. Contribution Agreement

Applicants of selected proposals will be invited to enter into a contribution agreement with DND. BOREALIS will work with the selected Lead Applicant to develop a contribution agreement, based on the proposed activities. Once an agreement is in place, the Lead Applicant becomes the Initial Recipient of funding and the Partner Organizations become Ultimate Recipients under the agreement. The agreement will set out the terms and conditions of the contribution, including the obligations of both parties, and the conditions under which payments will be made. These terms and conditions must also be reflected in the agreements signed between the Initial Recipient and the Ultimate Recipients.

The funding amount will be determined based on the overall eligible costs of the proposal, as well as the other sources of funding.

Applicants should note that until a written agreement is signed by both parties, no commitment or obligation exists on the part of DND to make a financial contribution to any proposal. Expenditures incurred or paid by the Applicants prior to the signing of such contribution agreement are ineligible.

All funded proposals will be announced on the IDEaS website.

10.Ongoing Considerations for DISH

10.1 Act Respecting the Ministère du Conseil Exécutif (M-30) for Québec Applicants

The Act Respecting the Ministère du Conseil Exécutif (M-30) may apply to an applicant that is a municipal body, school body, or agency located in the province of Québec. These applicants will be required to complete an additional information form and, if they are subject to the requirements of the Act, to obtain written authorization and approval from the Government of Québec prior to execution of any contribution agreement.

10.2 Basis of Contribution Payments

The Government of Canada's fiscal year runs from April 1 to March 31. The contribution agreement will specify the start and end dates for eligible costs, as well as the documentation required to support claims for payment.

Contribution payments will be made based on the receipt and approval of financial reports outlining actual eligible costs incurred, signed by the Recipient's Chief Financial Officer or another duly authorized officer. Payments will be tied to measurable, pre-defined milestones, as set out in the contribution agreement.

Where requested by the Recipient, advance payments may be permitted, subject to an assessment of financial need, risk level, and cash-flow requirements. To ensure appropriate financial oversight, a reasonable holdback, commensurate with funded activities' risk, may be applied to advance and progress payments. Holdbacks will be released once the conditions of the contribution agreement have been satisfied.

Recipients may be required to submit the following financial reports, as specified in the contribution agreement:

- Forecast reports, projecting eligible expenditures to be incurred in each fiscal year; and
- Actuals reports, summarizing eligible expenditures incurred and paid during the reporting period.

Advance payments may only be used to cover eligible costs (see Annex C – Eligible and Ineligible Costs). **Initial Recipients are expected to expend all funds received within the fiscal year for which they are provided**. Any unexpended advance may be treated as an overpayment and addressed in accordance with the overpayment provisions of the contribution agreement, including repayment or reduction of the contribution amount, together with applicable interest.

Recipients must retain and be prepared to provide supporting documentation for all eligible expenditures incurred.

Final payment will not be made until all agreed-upon activities have been completed and deemed acceptable by DND.

10.3 Redistribution of Funds

Approval by DND is required prior to the redistribution of funding by a Recipient to one or more individuals or entities.

Contribution agreement provisions will address the requirements of the Treasury Board Policy on Transfer Payments and the Terms and Conditions of the program. These Terms and Conditions must also be reflected in the agreements signed between the Initial Recipient and the Ultimate Recipients.

If an Initial Recipient redistributes funding to one or more Ultimate Recipients:

- the Initial Recipient has independence in the choice of Ultimate Recipients, with minimal guidance from DND, and will not be acting as an agent of the government in making distributions;
- the Initial Recipient contribution agreement will address the provisions set out in Appendix G (27 to 34) of the Directive on Transfer Payments; and

- Ultimate Recipients receiving redistributed funding must be approved eligible recipients and must utilize funding for the type and nature of eligible costs as defined in Annex C – Eligible and Ineligible Costs.

10.4 Research Security

In March 2021, the Government of Canada released a Research Security Policy Statement encouraging all members of the research community, including academia, private sector, and government to take extra precautions to protect the security of research, intellectual property, and knowledge development. Under this CFP, recipients are expected to actively identify, assess, and mitigate risks to research security in a manner proportionate to the sensitivity of the activities undertaken, the information involved, and the composition of proposed partners.

Research security risks may include, but are not limited to, foreign interference, unauthorized access to sensitive information, misuse of research outputs, and compromise of intellectual property or know-how. These risks should be considered across the full lifecycle of DISH activities, including partner selection, data access, personnel access, facilities, and information flows.

Applicants are not expected to eliminate all risk or only conduct classified research. Rather, applicants must demonstrate an understanding of relevant research security risks and describe reasonable, fit-for-purpose mitigation measures.

Canada is developing guidelines to integrate national security considerations into the evaluation and funding of research projects and partnerships. In the interim, recipients are responsible for undertaking appropriate due diligence and implementing mitigation measures commensurate with identified risks, rather than relying on future guidance.

When available, it is envisioned that the guidelines will be integrated in the due diligence assessment process undertaken by DND in support of research and development initiatives. In the meantime, recipients are encouraged 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. Recipients should conduct consistent and appropriate due diligence review of potential security risks to research activities and put in place timely measures to appropriately mitigate these risks.

DND may review proposed activities on national security grounds to ensure any national security risks are identified and addressed. DND reserves the right to request additional information, engage with recipients on risk mitigation measures, or apply appropriate conditions through the contribution agreement where necessary to address identified research security risks. In accordance with Research Security Guidelines, it may be necessary to share the information with Government of Canada departments and Agencies for the purpose of research security risk assessment.

Mandatory Research Security Plan

Applicants must submit a description of their **Research Security Plan** as part of their proposal (see part 6 in the proposal form). The Plan should describe:

- The research security risk profile of the proposed activities;
- Measures in place to mitigate identified risks;
- How data, knowledge, and research outputs will be protected and managed;
- How partnerships and collaborations are governed from a security perspective.

The Guidance for Research Organizations and Funders on Developing a Research Security Plan should be consulted for the development of the plan. The Research Security Plan will be assessed using a **risk-based and proportional approach** and will be evaluated as part of the mandatory criteria (see MC7 in Annex B).

10.5 Reporting Requirements

Specific reporting requirements will be defined in the Contribution Agreement. The DISH delivery model is based on active collaboration and continuous engagement. Each DISH will be assigned a **BOREALIS DISH Lead**, a DND subject-matter expert who will work closely and on an ongoing basis with the Recipient to monitor progress, support delivery, and ensure alignment with defence and security priorities. The DISH Lead will serve as the primary point of contact between the DISH and the Government of Canada defence and security community.

Regular working-level interactions between the Recipient, the BOREALIS DISH Lead will be established to enable timely issue identification, coordination, and decision-making throughout the period of performance.

In addition to ongoing engagement, DND will require the Recipient to submit formal progress reports to support program oversight and accountability. At a minimum, Recipients will be required to provide:

- Three (3) Progress Reports per fiscal year – 1 verbal and 2 written. An example of information requested within the Progress Reports may include the following:
  - Status of activities and progress toward DISH objectives and milestones
  - Progress toward securing physical and/or digital facilities, where applicable
  - Summary of technical, operational, or integration advancements enabled through the DISH
  - Description of experimentation, testing, integration, or validation activities conducted
  - Nature and extent of collaboration with DND/CAF and other defence and security stakeholders, including engagement with intended end users
  - Number and nature of partnerships and collaborations established or sustained
  - Leveraging of funding, including additional cash or in-kind contributions
  - Support to highly qualified personnel and skills development
- Forecast of Cash flow Requirements and Record of Expenditures/Actuals Report (semi-annual or quarterly).

DND may request that other performance measurement metrics be provided.

10.6 DISH Collaboration with Defence and Security Stakeholders

DISHs are expected to function as active collaboration environments for the Department of National Defence (DND), the Canadian Armed Forces (CAF), and other defence and security stakeholders.

Funded DISHs must be prepared to host and engage DND/CAF personnel as part of normal hub operations, including working-level collaboration, site visits, demonstrations, experimentation, testing, integration, and validation activities, as appropriate to the challenge area and security context.

As part of this expectation, DISHs should be prepared to:

- Provide access to DISH facilities and/or digital environments for DND/CAF personnel, subject to applicable security and access requirements
- Demonstrate how collaboration with defence and security stakeholders, including other federal government innovation programs, is embedded in DISH governance, operations, and activities

- Showcase progress in establishing and operating secure environments, including advancement toward security accreditation, where applicable
- Highlight how DISH activities are informing, supporting, or advancing defence and national security missions

In planning their proposed activities and budgets, applicants should account for the resources and effort required to support regular engagement with defence and security stakeholders, including preparation, and follow-up activities associated with such engagements.

10.7 Communication Activities

Communication activities related to Defence Innovation Secure Hubs (DISHs) must be conducted in a manner that is appropriate to defence and national security contexts, recognizing the sensitive nature of DISH activities and collaborations.

DISHs may undertake communications activities to support transparency, stakeholder awareness, and engagement with relevant audiences, where appropriate and consistent with security requirements. Such activities may include public-facing materials, presentations, demonstrations, or other communications related to DISH operations or outcomes.

Prior to any public release, publication, or external communication arising from DISH activities, the Lead Applicant must provide advance notification and relevant materials to BOREALIS, in accordance with the Contribution Agreement. This review is intended to assess whether proposed communications may contain information that is sensitive or prejudicial to national security, and to determine whether mitigation measures are required.

Public communications produced as part of a funded DISH must acknowledge the Government of Canada’s contribution, in accordance with guidance provided by BOREALIS, including use of approved acknowledgement and branding elements. The Recipient must make reasonable efforts to notify BOREALIS at least fifteen (15) working days in advance of any planned public communication, unless otherwise specified in the Contribution Agreement.

Where feasible and appropriate, communications may be made available in both official languages.

10.8 Intellectual Property

Unless otherwise specified in the Contribution Agreement, intellectual property (IP) generated in the course of activities funded under this program shall vest in the party that creates it, whether the Recipient or any participating partner.

The Recipient will be responsible for ensuring that appropriate IP arrangements are in place among all participating organizations, consistent with this principle.

Canada may, at its sole discretion, include a provision in the Contribution Agreement requiring that the Recipient grant Canada, in perpetuity, a non-exclusive, irrevocable, royalty-free and world-wide license, to use or have used, the intellectual property for government purposes. This license allows Canada to do anything that it would be able to do if it were the owner of the IP, other than exploit it commercially, or transfer or assign ownership of it.

10.9 Conflict of Interest

The Recipient and any participating partners are expected to identify, manage, and mitigate any actual, potential, or perceived conflicts of interest in accordance with their respective organizational policies and applicable laws and regulations.

If selected for funding, the program may request documentation demonstrating that the Recipient and, where appropriate, participating partners are aware of and have considered any actual, potential, or perceived conflicts of interest in accordance with their internal conflict of interest guidelines or governance frameworks.

The Contribution Agreement will include Conflict of Interest provisions requiring the Recipient to promptly notify DND of any actual, potential, or perceived conflict of interest that arises during the course of the funding period, and to take appropriate measures to address such conflicts to the satisfaction of DND.

10.10 Audit Rights

The Recipient must:

- keep proper accounts and records regarding the funded activities, for at least six (6) years after the agreement completion date;
- permit Government of Canada representatives to audit, inspect and make copies of those accounts and records at all reasonable times, up to six (6) years after the agreement completion date;
- grant the Government of Canada's authorized representatives access to audit and inspect the qualifying DISH and related facilities;
- furnish the Government of Canada's authorized representatives with such information as they may from time to time reasonably require with reference to the documents referred to herein; and
- promptly refund to DND any overpayments of the contribution disclosed by an audit, no later than thirty (30) calendar days from the date of Canada's notice.

Annex A – Challenge Statement

Defence Innovation Secure Hubs – Uncrewed Systems (UxS) and Quantum Technology

Canada's defence and national security organizations are operating in an environment characterized by rapid technological change, increasing system complexity, and heightened security requirements. Frontier technologies, like uncrewed systems (UxS) and quantum, are expected to have a significant impact on future defence and security operations; however, while testing and experimentation environments exist, few are suitable for work involving sensitive military applications. Despite rapid innovation in the commercial and research sectors, the absence of trusted conditions for development, integration, and demonstration limits the translation of promising UxS and quantum technologies into operationally relevant capabilities. Without mechanisms that enable controlled experimentation and trusted collaboration at the required classification level, Canada risks delayed adoption and reduced operational advantage as these technologies mature globally. This challenge seeks to address this gap by enabling conditions that support the development, integration, and demonstration of UxS and quantum technologies for defence purposes.

What BOREALIS provides

Approximately $50 million, across two streams (UxS and quantum), provided through the IDEaS program as non-repayable contributions, to support the establishment and secure enablement of existing facilities as DISHs in the UxS or quantum domains, and to advance innovation and stimulate collaboration.

What innovators bring

A consortium comprising at least two eligible partners, bringing existing facilities, strong connections to local innovation ecosystems, and the capability to deliver a coherent program of research and development in the uncrewed systems (UxS) or quantum domains, co-developed with consortia partners and their ecosystem, as defined in the challenge statements for each stream below. Consortia are expected to secure and operate these facilities as Defence Innovation Secure Hubs (DISHs), and to leverage partnerships across industry, academia, government, and the not-for-profit sector to support collaborative R&D, knowledge exchange, and technology advancement aligned with defence and security needs.

Uncrewed Systems (UxS) Stream

The Challenge

Uncrewed and counter-uncrewed systems (UxS and c-UxS) are rapidly transforming the character of modern military operations. While commercial and academic research and innovation in this domain advances quickly, significant gaps remain in the ability to develop, integrate, and mature UxS and c-UxS technologies that are resilient, interoperable, and effective in contested defence and security environments. The DISH seeks to accelerate the transition of promising UxS and c-UxS technologies into defence-relevant capabilities by enabling focused research, development, integration, and demonstration activities aligned with evolving operational needs in a secure environment.

Background and context

The growing availability, affordability, and capability of UxS platforms presents opportunities and challenges for DND/CAF and national security partners. International peers are increasingly pursuing a mix of high-end, survivable uncrewed platforms and more numerous, lower-cost systems, moving away from exclusive reliance on crewed platforms toward integrated networks of autonomous and semi-autonomous systems capable of operating in contested, degraded, and harsh environments. These trends span air, land, and multi-domain applications. At the same time, rapid advances by potential adversaries risk outpacing existing c-UxS capabilities. Addressing these challenges requires coordinated research and development across multiple domains and technical lines of effort, including uncrewed aerial and ground systems.

Expected Outcomes

The UxS DISH is expected to strengthen made-in-Canada solutions with sovereign and scalable supply chains for DND/CAF and other security partners by enabling and conducting research and development projects, with a focus on projects in Technology Readiness Levels 4-9, to mature, validate, test, and integrate UxS and c-UxS technologies into operationally relevant capabilities, supporting greater resilience against evolving adversarial capabilities. Areas of focus may include, but are not limited to:

- **Spectrum Dominance** – Ensuring freedom to operate across or without the electromagnetic spectrum, supporting UxS objectives and denying adversaries the same capability. This includes advancements in electronic warfare, command and control resilience, and robust data links and networking.
- **Awareness**– Multi-sensor systems that enable distributed sensing, onboard Detect and Avoid (DAA) systems, situational awareness, multi-UxS coordination, target acquisition, and target tracking through advanced fusion of sensors such as, but not limited to, acoustic arrays, electro-optical sensors, laser rangefinders and designators, and radio frequency detection systems.
- **Persistence**– Maximize operational time, range, speed, payload, and operational flexibility through options such as hybrid-electric propulsion, high-density power and energy systems, weight, routing, and other optimizations; Increase the resilience of UxS in challenging environmental conditions, such as the arctic; and support operations in contested environments with limited supporting infrastructure.
- **Interoperability** – Ensuring that UxS function with high levels of safety, reliability, and performance, including within human–machine teams and alongside crewed platforms, and across a range of ground and aerial infrastructure, payloads, and launch and recovery systems. This includes integration with relevant airspace and ground management frameworks, human factors research, autonomy assurance, and reliability testing.
- **Autonomy, Decision Support, and Battlefield Effects** – Approaches that enable trusted autonomous behaviours, decision support functions, and autonomous effects across all operational domains. This includes advanced human–machine interfaces, mission-level autonomy, adaptive decision-making in degraded or contested environments, and autonomy-enabled battlefield effects (including kinetic and non-kinetic actions) to contribute to offsetting the personnel shortages facing the CAF and national security partners. Trusted autonomy requires the development of validated trust, safety, and assurance frameworks that ensure autonomous systems can reliably deliver mission-critical effects.
- **Multi-UxS C2 and Coordinated Effects** – Future UxS-based force-multiplication requires solutions to enable effective human-machine teaming such that operators can intuitively and efficiently

command and control large sets of heterogeneous autonomous systems (1: many) through human-understandable, goal-based instructions. These solutions must allow heterogeneous UxS to interpret human intent; plan and direct activity individually or collectively; coordinate collaboratively across domains; and act autonomously within the battlespace. Emerging operational concepts increasingly rely on multiple heterogeneous UxS working together to produce combined effects (for example, long-endurance UAS providing targeting guidance for FPV munitions or navigation support to UGVs). Achieving these coordinated effects demands advances in algorithms, human-machine interfaces, and communication technologies for cooperative uncrewed operations.

- **Advanced Manufacturing** – Advanced sovereign and scalable production methods to optimize system performance through supply chain resilience, production volume, and rapid redesign. The design and production system should ensure parts supply redundancy, accommodate large changes in production demand, respond rapidly to theatre-driven design changes, and enable easy repair of UxS and c-UxS in theatre.

Quantum Stream

The Challenge

Quantum technologies have the potential to fundamentally alter sensing, communications, computing, and navigation in defence and security contexts. While significant advances are occurring globally, defence-relevant quantum capabilities face unique barriers related to sensitivity, security, integration, and testing. This challenge seeks to accelerate the maturation and application of quantum technologies that are critical to defence and national security by enabling focused research, development, integration, and demonstration activities within trusted environments.

Background and Context

Quantum technologies are an emerging and highly sensitive class of technologies with significant implications for defence and security. As geopolitical competition in quantum intensifies, Canada must treat quantum capabilities as a strategic and sovereign asset, essential to maintaining operational advantage and protecting critical defence and security systems. At the same time, many promising quantum technologies face challenges in transitioning from laboratory research to defence-relevant applications, particularly where secure facilities, system-level integration, and realistic testing are required.

Expected Outcomes

The quantum DISH is expected to strengthen Canada's defence and security posture by advancing quantum technologies toward operational relevance and reducing the risk of technological surprise. Proposals should contribute to the maturation of defence-relevant quantum capabilities through activities such as system integration, ruggedization, testing and evaluation (including field testing where appropriate), and demonstration, where these are necessary to address defence and security needs. Areas of focus may include, but are not limited to:

- **Quantum Sensing –** Quantum-enhanced radar, lidar, and imaging technologies that provide sensitivity, accuracy, resilience, covertness, or qualitatively new sensing effects beyond what is achievable with conventional sensing approaches, supporting detection and situational awareness in contested or denied environments.

- **Alternative Positioning, Navigation and Timing (PNT) –** Quantum-enabled sensing and timing approaches that support navigation or time distribution in GNSS-denied, degraded, or contested environments, including integration with existing platforms, systems, and operational workflows.
- **Quantum Computing and Algorithms –** Quantum and hybrid quantum–classical computing approaches, including algorithms, software tools, and workflows (including the integration of quantum computing and AI), that enable defence-relevant analysis, modelling, simulation, optimization, and decision-support tasks, as well as the rapid design and discovery of defence-relevant materials, devices, or medical countermeasures, and their validation through synthesis, testing, and demonstration where appropriate.
- **Quantum Communications and Networking –** Technologies and network architectures that support quantum communications and networking, including quantum key distribution and the integration of terrestrial, airborne, and space-based quantum communication systems.

Annex B – Evaluation Criteria

Applicants must complete the DISH Proposal form with sufficient detail to enable Canada to assess the proposal against the established evaluation criteria. The information provided should clearly demonstrate how the proposal meets each criterion.

Proposals will be assessed using mandatory criteria (MC) and Point-rated criteria (PRC).

To be eligible for funding, proposals must meet all mandatory criteria. The responsibility lies with the Applicant to demonstrate that the proposal clearly meets each criterion.

Mandatory Criteria (MC)

Criteria	Evaluation Matrix (Pass / Fail)
MC1 – Applicant Eligibility	**Pass:** The applicant must be a legal entity duly incorporated under Canadian federal or provincial law and validly existing in Canada, including: • Canadian universities and other post-secondary institutions chartered in Canada • Incorporated Canadian not-for-profit organizations or associations • Incorporated Canadian for-profit companies, organizations, or associations **Fail:** The applicant is **not** a legal entity duly incorporated under Canadian federal or provincial law and validly existing in Canada as listed above; **or** is a federal department, federal agency, Crown corporation, **or** a provincial/territorial or municipal government organization.
MC2 – Minimum Partnership Composition	**Pass:** The proposal must identify, at a minimum, partners from at least two (2) separate eligible organizations and/or institutions; and the role of each partner is described at a high level, demonstrating how each contributes to delivering the objectives of the proposed Defence Innovation Secure Hub (DISH). **Fail:** One or more required partners are not identified; **or** partners are identified in name only with no described role in the proposed DISH.
MC3 – Alignment with DISH Objectives	**Pass:** The proposal must address the core intent of the DISH Call for Proposals, with defence- or security-relevant research, development, and/or experimentation as its primary purpose, and must align with one or more priority domain(s) identified in the Call (quantum or uncrewed systems). **Fail:** The proposal does not address the DISH objectives, is off-topic, or is primarily commercial, civilian, or infrastructure-only in nature.

MC4 – Eligible Activities, Costs, and Funding Limits	**Pass:** The proposed activities must be eligible under the DISH Call for Proposals, and the proposed budget must comply with all funding limits, including: • Capital expenditures not exceeding 50% of total eligible costs • Administrative/overhead costs not exceeding 15% of total eligible costs **Fail:** The proposal includes ineligible activities or costs, or exceeds one or more funding limits.
MC5 – Physical Infrastructure Identification and Readiness	**Pass:** The proposal must identify the physical infrastructure to be used for the DISH and include a high-level plan demonstrating that the infrastructure exists and/or can be made available and appropriately fitted up and secured within the funding period. **Fail:** The proposal does not identify physical infrastructure, or the infrastructure is purely conceptual.
MC6 – Feasibility Within the Funding Period	**Pass:** The proposal must include a high-level workplan demonstrating that major research, development, experimentation, and hub activities can be completed by 31 March 2028. **Fail:** No workplan is provided, or hub activities clearly extend beyond the funding period without justification.
MC7 – Research Security Plan	**Pass:** The proposal includes a high-level Research Security Plan that is demonstrably aligned with the Government of Canada's Guidance for Research Organizations and Funders on Developing a Research Security Plan. **Fail:** The proposal does not include a Research Security Plan, or the plan fails to address the federally defined components of a Research Security Plan as set out in the Guidance for Research Organizations and Funders on Developing a Research Security Plan.

Point-Rated Criteria (PRC)

A point scale is utilized to assess the rated criteria. If the proposal provides insufficient or no information for any of the criteria, it may result in a failing score or zero points being awarded.

Rating scale:
Insufficient: 0 points

Poor: 1 point
Fair: 3 points
Good: 6 points
Excellent: 10 points

Collectively, the point-rated criteria assess defence relevance, delivery quality, collaboration, infrastructure enablement, value for money, inclusivity, and the sustainability of DISH capabilities.

Criteria	Evaluation Criteria
PRC1 - Defence and Security Relevance	Applicants must clearly demonstrate the defence and/or security relevance of the proposed DISH. This includes articulating the defence or security problem space and intended user context, demonstrating that proposed R&D and experimentation activities are tightly linked to that problem space, showing relevance to the priority domain(s) identified in the Call for Proposals, and describing a plausible pathway from R&D activities to defence use, experimentation uptake, or capability adoption.
PRC2- Quality and Coherence of the R&D Program	Applicants must provide a coherent and well-structured R&D and experimentation program. This includes clearly defined and measurable objectives, a logical sequencing of activities, defined outputs or deliverables, identification of key technical risks and mitigation strategies, and a scope that is ambitious yet credible given the funding, facilities, and timeframe.
PRC3 - Delivery, Governance, and Execution Capacity	Applicants must demonstrate a delivery and governance approach capable of operating a Defence Innovation Secure Hub and executing multiple concurrent R&D efforts. This includes clear decision-making structures, defined roles and accountabilities across partners, a credible operational management approach, and evidence of relevant experience delivering complex, multi-partner initiatives. This also includes identification of key schedule risk and mitigation strategies, as part of a credible plan to spend the full proposed budget within the proposed timeframe.
PRC4 - Collaboration Model and Partner Integration	Applicants must demonstrate meaningful integration of partners in the execution of R&D and experimentation activities. This includes showing that all partners are embedded in delivery roles, that collaboration mechanisms enable effective knowledge transfer, and that intellectual property, data, and access arrangements have been considered at an appropriate level for the scope of work.
PRC5 - Infrastructure and Security Enablement Quality	Applicants must demonstrate that the proposed infrastructure and security enablement are well matched to the R&D and experimentation activities. This includes suitability of facilities, credibility of any phased security evolution, and the ability of the infrastructure to support agile, multi-user experimentation.

PRC6 -Value for Money and Co-Investment	Applicants must demonstrate that the proposed budget represents value for money and is aligned with delivering R&D and experimentation outcomes. This includes prioritization of R&D activities, justification of infrastructure expenditures, efficient allocation of resources across partners, and, where applicable, credible and additive co-investment that strengthens the proposal.
PRC7 - Sustainability	Applicants must identify DISH capabilities expected to have value beyond the funding period and describe a credible approach to sustaining or transitioning those capabilities after funding ends. This includes alignment of post-funding use with defence and security objectives.
PRC8 -GBA+ and Inclusive Access	Applicants must describe how GBA+ considerations have been addressed in a manner proportionate to the scope of the proposal. This includes consideration of inclusive participation and equitable access to DISH capabilities, including how eligible industry, academic, and other stakeholders can reasonably access and participate in DISH activities, consistent with security, safety, and operational requirements.

Annex C – Eligible and Ineligible Costs

Eligible costs are limited to the following categories.

1. Salaries and benefits

Salaries and benefits are eligible if they are directly related to DISH activities, including project management, and reflect the exact costs associated with payment of salary and benefits.

- Salaries: not to exceed $250,000 per full-time equivalent (excluding benefits). This maximum applies to all positions (including employment contracts) and shall be pro-rated on the basis of the proportion of time worked relative to the full-time equivalent.
- Benefits: not to exceed 25% of salaries per full-time equivalent.

Benefits are defined as employment costs paid by the employer and may include the following:

- Employer's portion of CPP/QPP
- Employer's portion of Employment Insurance (EI)
- Employer's portion of group insurance
- Employer's pension contributions

2. Professional services (provided by third parties not affiliated with the recipient)

Eligible professional services include work performed by external experts, consultants, or service providers who are contracted specifically to provide specialized knowledge, expertise, or technical services that are directly required to carry out the approved project.

It is the responsibility of the recipient to ensure that all costs from service providers providing contracted services are eligible costs. Upon request, recipients will provide DND a copy of contracts for services under the DISH.

The DISH Contribution Agreement should not be used or replicated for contracting with other parties. A recipient's own contract should detail the activities and outcomes to be achieved under that contract, the costs, and deliverables.

Note: specific professional services related to the fit-up of existing facilities shall be considered to fall under the facilities sub-category of *4. Capital Expenses (equipment and facilities)* and are thus included under the 50% cap on total eligible proposal costs that can be dedicated to fit-up of existing facilities.

3. R&D expenses

Eligible R&D expenses include costs directly attributable to the conduct of basic and applied research addressing defence and national security challenges identified in the DISH's R&D plan.

R&D expenses may include, but are not limited to:

- Materials and supplies: small system components, electronics, and any other materials that are being integrated into prototypes or consumed during R&D activities. Also includes stock materials that are used to manufacture components on site.
- Prototyping: Expenses related to the development of solution prototypes and systems, validation and integration, testing and evaluation.

- Data acquisition and analysis: Costs associated with data collection, acquiring necessary datasets, testing environments, modelling tools, and analytical software required to support R&D objectives. Costs associated with obtaining access to research literature, such as scientific journals and information databases, used for the delivery of the DISH's R&D plan are eligible under this sub-category.
- Travel: Travel costs necessary for conducting research, collaboration with DND/CAF stakeholders, field testing, or technical reviews, where directly related to R&D activities. Travel expenses must be incurred in accordance with the National Joint Council travel directive.

4. Capital expenses (equipment and facilities)

Equipment is defined as any item (or interrelated collection of items comprising a system) which is used wholly or in part for the research proposed and meets all three of the following conditions:

1) non-expendable tangible property;
2) having a useful life of more than one year; and,
3) a cost of $2,000 or more.

Note: An item that fails to meet all three conditions listed above could be classified as materials and supplies (see *3. R&D Expenses* above).

The Recipient will be responsible for obtaining the fair value of equipment at the time of purchase.

Eligible costs under the facilities sub-category include modifications, upgrades, and fit-up of existing facilities required to enable secure collaborative work up to Level II (Secret), such as physical security enhancements, access controls, secure rooms, and supporting infrastructure.

- Costs must be directly related to enabling DISH activities.
- Fit-up costs must not exceed 50% of total approved eligible costs.
- New construction, including additions to existing buildings, is not eligible.

5. Administrative overhead

Administrative Overhead costs are indirect expenditures incurred by recipients, which are required for the DISH establishment and/or research activities, but cannot be specifically identified as direct costs. These costs relate to the use of the organization's resources, which may include, but are not limited to:

- Administrative support (e.g. accounting, payroll administration, meetings);
- Information Technology support;
- Internet, telephone, excluding long-distance charges;
- Use of photocopiers, fax machines, and other office equipment;
- Use of existing workstations, including furnishings and equipment (e.g. computers, scanners);
- Normal office software (not including software specifically required for the project);
- Memberships and subscriptions only if required to complete project activities;
- Staff recruitment and training;
- Routine laboratory and field equipment maintenance (e.g. oil changes);

- Building occupancy and operating costs (i.e. use of space); and,
- Facilities maintenance.

The administrative overhead costs cannot exceed 15% of the total Eligible Expenditures (before overhead).

6. Securing Intellectual Property

Eligible expenses include costs directly associated with protecting, securing, and managing IP that arises from funded activities.

Eligible IP costs may include, but are not limited to p**atent costs:**

- Preparation and filing of patents related to DISH outcomes.
- Patent prosecution fees (e.g., official government filing fees).
- Patent searches and novelty assessments.

Ineligible Costs include, but are not limited to, the following:

- Salaries and benefits for researchers receiving direct and continuous salary through universities or other post-secondary institutions;
- In-kind contributions;
- Professional training or development, such as computer or language courses;
- The purchase of land or buildings;
- Costs of moving a lab;
- The purchase or lease of private/personal vehicles, vehicle maintenance costs or “Rental” charges for company-owned vehicles;
- Assets and capital items not specifically required for the execution of DISH activities;
- Normal costs of establishing a commercial operation;
- Costs for activities that are deemed to be part of normal business practice for any Recipient, such as: Review engagements and audits, unless required in the agreement, Board of Directors’ meetings, Insurance;
- Depreciation;
- Interest or overdraft charges and credit card fees;
- Refundable portion of the GST/HST, value-added taxes, or other items for which a refund or rebate is receivable;
- Hospitality – such as catering, alcohol, entertainment, honorariums, gifts (e.g., gifts for speakers or facilitators);
- Monthly parking fees for vehicles, unless specifically required for field work;
- Costs of regular clothing;
- Membership fees, unless specifically required for the execution of funded activities and the DISH partners do not already have membership;

- Discretionary employee benefits (e.g., parking at employer’s location, relocation costs for employees hired for the DISH, supplementary employment insurance benefits for maternity/paternity leave, staff awards and recognition);
- Costs for activities intended to directly influence/lobby governments;
- Direct marketing, business promotion or one-on-one extension types of activities;
- Costs associated with the review of graduate and PhD theses; and,
- Other costs not specifically required for the DISH.