



DEFENCE READINESS PROGRAM

APPLICANTS GUIDE

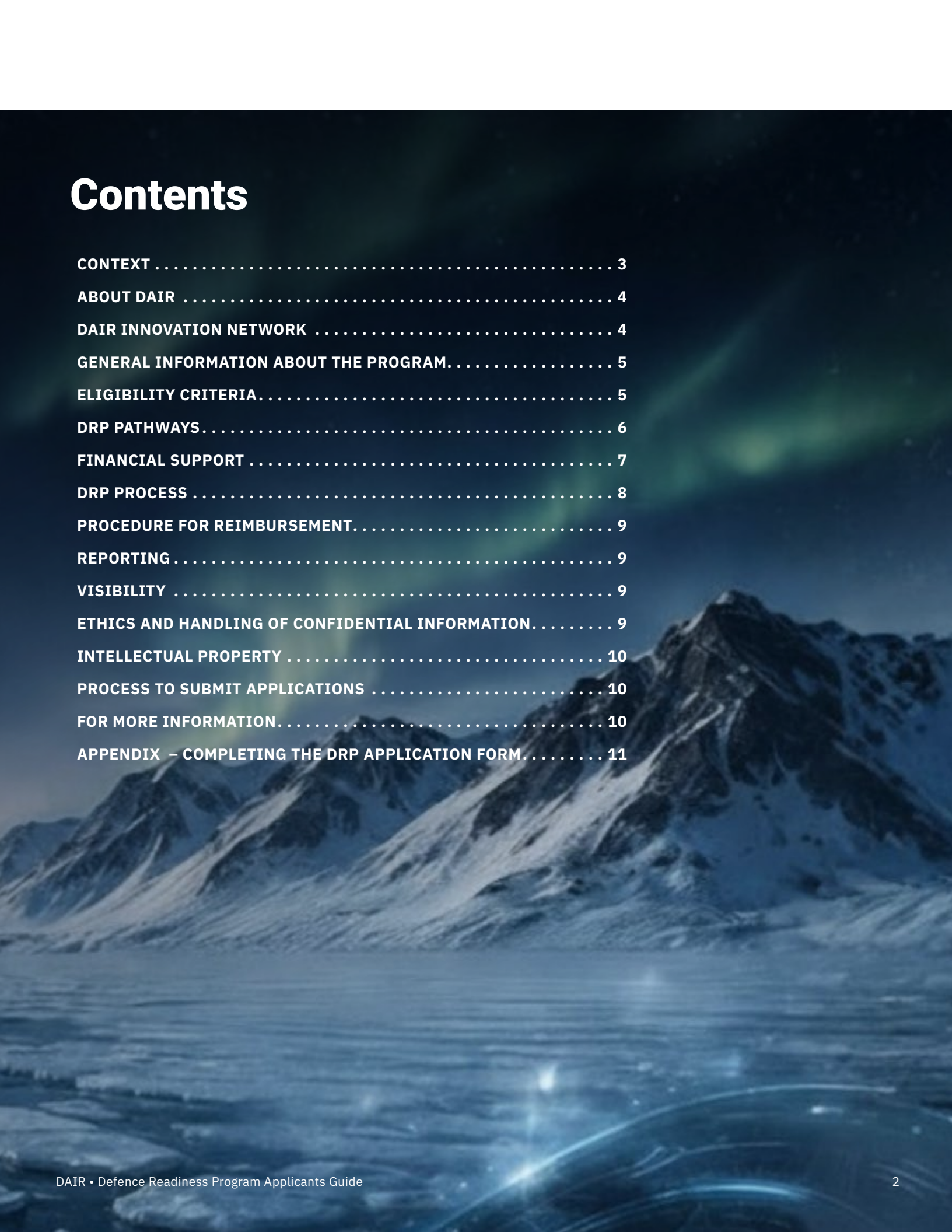
JULY 2026



DAIR

DOWNSVIEW AEROSPACE | DOWNSVIEW AÉROSPATIALE
INNOVATION & RESEARCH | INNOVATION & RECHERCHE

Ontario 



Contents

- CONTEXT 3
- ABOUT DAIR 4
- DAIR INNOVATION NETWORK 4
- GENERAL INFORMATION ABOUT THE PROGRAM..... 5
- ELIGIBILITY CRITERIA..... 5
- DRP PATHWAYS..... 6
- FINANCIAL SUPPORT 7
- DRP PROCESS 8
- PROCEDURE FOR REIMBURSEMENT..... 9
- REPORTING..... 9
- VISIBILITY 9
- ETHICS AND HANDLING OF CONFIDENTIAL INFORMATION..... 9
- INTELLECTUAL PROPERTY 10
- PROCESS TO SUBMIT APPLICATIONS 10
- FOR MORE INFORMATION..... 10
- APPENDIX – COMPLETING THE DRP APPLICATION FORM..... 11

Context

Canada's aerospace and defence sector is entering a period of significant growth and transformation. Increased investments in national defence, commitments to strengthen continental security through NORAD modernization, evolving NATO spending objectives and the implementation of Canada's Defence Industrial Strategy are creating new opportunities for Canadian companies to participate in domestic and international defence supply chains.

At the same time, the expectations placed on defence suppliers continue to evolve. Government customers, Original Equipment Manufacturers (OEMs) and Tier-1 suppliers increasingly require organizations to demonstrate robust cybersecurity practices, security clearances, organizational governance, and the ability to safeguard sensitive information, intellectual property and critical technologies. For many organizations, defence readiness has become a prerequisite for participating in defence markets rather than simply a competitive advantage.

Ontario is home to a diverse and highly capable network of aerospace and advanced manufacturing small- and medium-sized enterprises (SMEs). Many of these companies possess world-class technical expertise, advanced manufacturing capabilities and innovative products that are well suited to defence applications. However, navigating the complex security, compliance and procurement requirements associated with the defence sector can be challenging, particularly for organizations entering the market for the first time or seeking to expand their defence business.

About DAIR

Downsview Aerospace Innovation & Research (DAIR) is incorporated federally as a not-for-profit organization, a consortium of aerospace companies and post-secondary institutions.

Headquartered at Downsview Park in Toronto, DAIR is building a nationally connected A&D Innovation Hub where organizations collaborate to develop, validate and commercialize new technologies, strengthen supply chains and create opportunities for Canadian industry.

DAIR's mission is to catalyze world-class innovation by facilitating collaboration within industry, academia and government to develop transformative technologies and a future-ready workforce. DAIR advances this mission by:

- Enabling access to state-of-the-art equipment and infrastructure to accelerate leading-edge research and technology adoption.
- Creating training solutions for business and technology challenges of today and tomorrow.
- Providing a platform for industry, academic and government to foster collaborative innovation.
- Supporting continuous improvement and innovation in the supply chain.
- Harnessing our collective voice to bring awareness to and promote the industry and innovation ecosystem locally, nationally and globally.

Today, DAIR operates from multiple partner facilities across the Downsview Innovation Hub, including the Bombardier Centre for Aviation and Aerospace at Centennial College, the Toronto Metropolitan University Centre for Advancing Engineering Research & Innovation in Aerospace (AERIAS), and the Landing Gear Innovation Lab, while continuing to expand its physical innovation infrastructure through new facilities currently under development.

DAIR Innovation Network

Companies are not required to be members of the DAIR Innovation Network when applying to the Defence Readiness Program (DRP). However, companies selected to participate in a DRP cohort will be required to join the DAIR Innovation Network upon execution of the funding agreement with DAIR. Membership is subject to the applicable annual fee and is renewable each year.

The DAIR Innovation Network brings together aerospace and defence companies, post-secondary institutions and ecosystem partners to foster collaboration, accelerate innovation and strengthen Canada's aerospace and defence ecosystem. Through the Network, members gain access to exclusive networking events, workshops, thought leadership activities, collaborative opportunities, strategic introductions and connections with industry, academia and government. Members also receive ongoing opportunities to showcase their capabilities, identify potential customers and partners and participate in initiatives that support business growth, innovation and competitiveness.

While the DRP provides targeted support to strengthen an individual company's defence readiness position, membership in the Innovation Network extends that value well beyond the life of the program by creating opportunities for long-term collaboration, new business relationships and continued engagement within Ontario's aerospace and defence community. For many SMEs, Innovation Network membership delivers a strong return on investment through the connections, visibility and collaborative opportunities it provides.

Applicants are encouraged to contact DAIR to learn more about the Innovation Network, its membership benefits and the applicable annual membership fee.

General information about the program

The DAIR Defence Readiness Program (DRP) was established to help Ontario SMEs build the organizational capabilities required to become trusted participants in Canada's defence industrial base. Through independent readiness assessments, tailored implementation roadmaps, expert guidance and funding, the program supports organizations as they strengthen their security, improve cybersecurity and organizational readiness, begin implementation of required compliance measures, and ultimately position themselves to pursue new defence opportunities.

The DRP recognizes that every organization begins its defence readiness journey from a different starting point. Some companies may already possess significant experience supporting defence customers and require assistance implementing specific improvements, while others may be entering the sector for the first time and need guidance to understand the security, cybersecurity and organizational capabilities required to compete successfully. The program is designed to provide flexible support that reflects the individual needs and objectives of participating SMEs.

Beyond supporting individual companies, the DAIR Defence Readiness Program contributes to strengthening Ontario's aerospace and defence ecosystem by helping develop a broader base of capable, secure and competitive suppliers. As more Ontario SMEs become defence-ready, Canada's industrial base becomes more resilient, supply chains become stronger, and Canadian organizations are better positioned to support government, OEMs and Tier-1 suppliers on current and future defence programs.

The DRP offers participating companies:

- A comprehensive assessment to evaluate current defence readiness.
- A tailored roadmap outlining the specific subsequent actions required to achieve defence readiness.
- Access to funding to support the implementation of recommended improvements.
- Ongoing support from DAIR, leveraging its network of defence experts to guide SMEs through their readiness journey.

Eligibility criteria

To be eligible, the applicant SME must fulfill the following requirements:

- Must be a small- to medium-sized enterprise (SME), that is, less than 500 full-time employees and operating a manufacturing facility.
- Must be an Ontario-based organization (or an Ontario-based subsidiary). Applicants that are U.S.-based businesses are not eligible. A U.S.-based business is any business (including a sole proprietorship, partnership, corporation or other business structure) that (i) has its headquarters or principal office located in the United States; and (ii) has fewer than 250 full-time employees in Ontario. If the applicant is a subsidiary of another corporation, criterion (i) is deemed to be met where the subsidiary is controlled by a corporation whose headquarters or principal office is located in the United States.
- Must be a current defence supplier or have intentions to work in the defence supply chain.
- The applicant must be in compliance with all federal, provincial, territorial, municipal and other applicable laws, including without limitation, statutes, regulations, by-laws, rules, ordinances and decrees.

Based on the number of applicants to the program, SMEs will be selected based on criteria including but not limited to type of company, size of the SME and number of employees. Please contact Verlyn Smith should you have any questions regarding eligibility.

After being accepted to participate, the SME must sign a formal funding agreement with DAIR. This agreement explains in detail your responsibilities to DAIR as part of the program.

DRP pathways

Organizations may participate through one of two pathways.

Pathway 1 – Assessment and Implementation

This pathway is intended for organizations that are new to the defence sector or require assistance determining their current level of defence readiness.

Participants begin with an independent readiness assessment conducted by DAIR's designated assessment partner. Following completion of the assessment, each organization receives a tailored roadmap identifying recommended implementation activities. Subject to DAIR approval, eligible implementation activities may then proceed with the remaining funding allocation.

Pathway 2 – Direct Implementation

Some organizations have already completed recognized readiness assessments or can demonstrate an appropriate level of existing defence readiness.

Where sufficient evidence exists, DAIR may determine that an additional assessment is unnecessary. These organizations may proceed directly to implementation activities, allowing them to focus program funding on projects that further strengthen their defence readiness.

DAIR reserves the right to determine whether existing documentation or evidence is sufficient to support entry into the Direct Implementation pathway.

DAIR has partnered with 123 Defence to support the DAIR Defence Readiness Program. 123 Defence represents an amalgamation of decades of military service, agile innovation, visualization and implementation, as well as over 35 years of experience in business software development and client services. They enable aerospace, defence, security and advanced manufacturing SMEs to meet security and certification requirements needed to win federal and defence contracts.

Their work includes: Security clearance enablement (DOS, DSC, FSC); Compliance (Protected B, Controlled Goods, CPCSC Level 2 aligned); Controlled Goods Program; Certification readiness including Canadian Program for Cyber Security Certification (CPCSC) Level 1 and Level 2 and Cybersecurity Maturity Model Certification (CMMC) Level 1 and Level 2; Fractional cybersecurity and certification support.

Regardless of the pathway followed, all participating organizations receive ongoing guidance from DAIR throughout the implementation process and are expected to complete approved activities within the timelines established in their Funding Agreement.

Projects must be completed within 6 months post assessment, or in the case of Direct Implementation, post-approval.

Submitted applications will be reviewed and approved applicants will be required to (1) enter into a contract with DAIR, (2) join the DAIR Innovation Network and (3) complete supported activities and report back to DAIR by the project deadline.

Financial support

The DAIR Defence Readiness Program provides non-repayable funding to support implementation activities that strengthen an organization's defence readiness.

Successful applicants may receive up to \$20,000 CAD in non-repayable funding. For SMEs through Pathway 1, the cost of the assessment and roadmap is a part of this total amount.

DAIR will contribute up to 75% of eligible project costs, to a maximum contribution of \$20,000 CAD (for projects that have a total of \$26,667 CAD or more). Participating SMEs are responsible for contributing remaining project costs. If the total project costs are less than \$26,667, DAIR's funding remains capped at 75%.

SMEs accepted into the program are required to submit an invoice to DAIR in the total of \$5000 CAD as their demonstration of commitment to participate. This deposit will be fully reimbursed upon successful completion of the program parameters.

Funding is intended to support implementation activities identified through the readiness assessment or otherwise approved by DAIR under the Direct Implementation pathway.

All proposed activities and associated budgets must be reviewed and approved by DAIR before project work begins. Expenses incurred prior to approval are not eligible unless expressly authorized by DAIR in writing.

Funding is provided on a reimbursement basis following satisfactory completion of approved activities and submission of all required reporting and supporting documentation, in accordance with the terms of the Funding Agreement

Other notes:

- DAIR reserves the right to limit the number of SMEs and funding provided.
- Project implementation funding may be accessible upon completion of the Assessment and sign off on project scope by DAIR (to ensure alignment with program parameters).
- The non-repayable contribution will be provided directly to the applicant SME. No funds will be transferred to a partner. The applicant SME has the sole responsibility to handle any contractual and financial matters with partners or consultants.
- The applicants must demonstrate that project activities are beyond the scope of regular operations.

Eligible activities could include:

- Consulting.
- Security screening costs.
- Cybersecurity software/hardware installation, implementation and training costs.
- Policy development.
- Salaries.
- Compliance certification or registration costs.

Ineligible activities (and costs) include:

- Routine operating costs.
- Capital expenditure.
- Activities not related to compliance.
- Consultant expenses such as travel/mileage, meals and accommodation.
- All expenses not submitted and approved in advance by DAIR.

Note that DAIR reserves the right to limit the proportion or amount of funding that may be allocated to salary expenses.

DRP process

- 1. Independent readiness needs assessment (as determined)** – to assist SMEs in identifying gaps and to determine the roadmap to participate in defence opportunities.
- 2. Assessment results and recommendations (if completing step 1)** – participants receive a summary of their assessment results, including identified gaps, risk areas, and recommended actions to move towards compliance.
- 3. Readiness project selection** – the organization selects a tailored readiness project outlining the activities required to address identified gaps. Upon approval of selected project, participants must sign a project charter to confirm project scope.
- 4. Project implementation** – the organization undertakes the approved readiness activities, in alignment with program requirements and timelines.
- 5. Project completion and reporting** – upon completion, the organization submits final deliverables and reports demonstrating that the required readiness activities have been completed and compliance objectives achieved. Eligible expenses are then reviewed, and approved funding reimbursement is processed in accordance with the Funding Agreement.

Procedure for reimbursement

1. Once the SME has submitted all documents required for reporting on projects within the DAIR DRP, the supplier may proceed to claim reimbursement for expenses incurred. DAIR reimburses 75% of total project costs, up to \$20,000 CAD.
2. SMEs will be required to forward an invoice and direct deposit information to DAIR for the amount to be claimed for the reimbursement, based on eligible and approved project costs.
3. SMEs must provide documentation issued by their Human Resources department to substantiate salary expenses. Such documentation must include the employee's name, hourly pay rate, total hours worked during the project implementation period, and the number of hours specifically attributed to project-related activities.
4. Receipts from the external service providers and proof of payment will be required to be submitted. Acceptable proof of payment should show SME name, service provider name, date of payment or transfer, payment amount and currency, and be issued by a financial institution such as a cashed cheque, a bank transfer, wire payment or credit card payment.

DAIR will review all documents received and reserves the right to request further or related documentation prior to accepting proof of payment.

Reporting

The DAIR team will work with the SME to ensure that baseline measures, where applicable, are collected to compare with post-implementation results.

A mid-way review will be scheduled to ensure that all projects are progressing according to the approved timeline.

As a final step of the DAIR DRP, the SME will advise the DAIR team of project completion and receive the Project Results Summary template. The SME will update the document with current company statistics and project results.

Visibility

Due to support of the DAIR DRP by the Government of Ontario, approved SMEs will be required to acknowledge the support received from DAIR and the Government of Ontario for the project in any communications, including websites, news releases, social media, success stories and announcements. All media and content must have DAIR approval before publishing.

Ethics and handling of confidential information

Information shared with DAIR will be held in confidence and within secure storage. Upon execution of an Agreement, the Parties shall keep confidential and shall not disclose the contents of the Agreement or the transactions contemplated, without the consent of all Parties, notwithstanding requirements to the Government of Canada under the Access to Information Act (Canada), the Privacy Act, the Library and Archives Act of Canada, and to the Government of Ontario through the Freedom of Information and Protection of Privacy Act (Ontario).

Upon entering into an Agreement with DAIR, the applicant will agree that DAIR is authorized to share information pertaining to the applicant, its application and its Funding Agreement with the Government of Ontario for the purposes of reporting requirements. Disclosure of this information is subject to the relevant privacy and confidentiality laws including, without limitation, the Freedom of Information and Protection of Privacy Act.

DAIR requires any company entering into an Agreement for the DAIR SDI to maintain proper and accurate accounts and records of the project for a minimum of six (6) years after the date of completion of the project. The applicant understands that the Government of Ontario will maintain a right to audit the accounts and records of recipients with respect to the funded project.

Applicants are expected to conduct all activities related to their application and any resulting funding agreement in a manner that is objective, impartial and free from conflicts of interest.

For the purposes of this program, a conflict of interest includes any circumstance where the applicant, or any individual with the ability to influence the applicant's decisions, has outside commitments, relationships or financial interests that could, or could reasonably be perceived to, interfere with the objective, unbiased and impartial management of the proposed project or the use of program funding.

Applicants must disclose to DAIR any actual, potential or perceived conflict of interest that exists at the time of application or that arises during the term of the project. DAIR reserves the right to determine whether a disclosed conflict may affect the applicant's eligibility or whether appropriate mitigation measures can be implemented. Failure to disclose a conflict of interest may result in an application being deemed ineligible, the withdrawal of funding, or termination of a funding agreement.

Applicants are also responsible for ensuring compliance with all applicable legislation, regulations and ethical obligations related to lobbying, procurement and conflicts of interest.

Intellectual property

DAIR will not take ownership of or any other rights in any Intellectual Property arising from any project supported under the DAIR SDI.

Any Intellectual Property stemming from a supported DAIR SDI project shall be owned by the applicant, the project partners, or an entity based in Canada for the duration of the Funding Agreement plus six (6) years.

The applicant shall make all reasonable efforts to exploit the IP generated from this funding in Canada for the duration of the funding Agreement plus six (6) years.

Process to submit applications

To submit applications, SMEs are required to complete, sign and submit the DAIR DRP Application Form, as well as any other required documents. The application can be downloaded from DAIR's website at the following link:

dairhub.com/initiatives/dair-defence-readiness-program/

The DAIR DRP Application Form must be submitted via email to: verlyn.smith@dairhub.com

Intake will remain opened until the program is fully subscribed.

For more information

For any additional questions, please contact Verlyn Smith, DAIR Industry Development & Readiness Manager

Appendix – Completing the DRP Application Form

This portion of the guide explains how to complete the DRP Application Form and supporting documentation. It is intended to help Ontario SMEs prepare a complete, accurate and timely submission.

How to Complete the Application

The DCRP application form consists of six sections. The following describes how to complete each section and what information to prepare.

SECTION 1 – General Information

Provide basic eligibility information including:

- Confirmation that your business is engaged or intends to engage in defence industry opportunities.
- Acknowledgement that DAIR may request supplementary documentation.

SECTION 2 – Applicant Information

Prepare the following company details:

Business Identity

- Legal business name.
- Operating name (if different).
- Business structure (e.g., corporation, sole proprietorship, partnership).
- Public or private company designation.

Corporate and Contact Information

- Headquarters address.
- Additional locations (if any).
- Whether the company is part of a larger corporate group; if yes, list parent company name and full address.
- Incorporation date.
- Number of permanent employees at applicant location.
- CRA 9 digit Business Number.
- First 3 digits of NAICS code.
- Company website.
- Full address (street, unit, city, province, postal code).
- Phone number.

Contact Information

Principal

Enter the name, job title, phone number and email address for the contact within your organization who will sign the application.

Project Manager

Enter the name, job title, phone number and email address for the contact within your organization who will be the point of contact for DAIR and the assessing organization. This contact will be responsible for the following but not limited to providing project updates, documents required, invoices and proposals.

Appendix – Completing the DRP Application Form (cont'd)

SECTION 3 – Compliance Status

A) CURRENT CERTIFICATIONS / AUTHORIZATIONS

Select all certifications your organization already has:

- Reliability Status.
- Designated Organization Screening (DOS).
- Document Safeguarding Capability (DSC).
- Facility Security Clearance (FSC).
- Controlled Goods Program (CGP).
- Canadian Program for Cyber Security Compliance (CPCSC) – Level 1 or 2.
- Cybersecurity Maturity Model Certification (CMMC) – Level 1 or 2.
- ISO 27001.
- NIST 800 171.
- Other (specify).
- None.

B) READINESS OBJECTIVES

Indicate the compliance designations your organization is interested in pursuing.

• Reliability Status:

What it is: A basic personnel security screening conducted by the Government of Canada.

Who needs it: Employees who require unsupervised access to protected government information or worksites (Protected A/B).

Scope: Identity verification, criminal record check, employment verification.

Typical use: Entry level government contracts or access to non classified sensitive info.

• Designated Organization Screening (DOS)

What it is: An organizational security screening under the Government of Canada's Contract Security Program (CSP).

Who needs it: Companies bidding on federal government contracts that involve protected information.

Scope: Assesses ownership, internal security controls and key personnel reliability.

Typical use: Prerequisite for many Public Services and Procurement Canada (PSPC) contracts.

• Document Safeguarding Capability (DSC)

What it is: Authorization to store and safeguard protected or classified government documents at your facility.

Who needs it: Organizations handling Protected A/B or Classified material.

Scope: Physical security (locks, safes), handling procedures, staff training.

Typical use: Consulting firms, engineering firms, defence contractors.

• Facility Security Clearance (FSC)

What it is: A higher level facility approval under the CSP.

Who needs it: Organizations working with Classified (Confidential, Secret, Top Secret) info.

Scope: Facility security, IT security, cleared personnel and governance controls.

Typical use: Defence, intelligence, aerospace, national security contracts.

• Controlled Goods Program (CGP)

What it is: A mandatory program regulated by Public Services and Procurement Canada.

Who needs it: Organizations handling controlled military or strategic goods, including technical data.

Scope: Personnel screening, security plans, access control, record keeping.

Typical use: Defence manufacturing, aerospace, dual use technology companies.

• Canadian Program for Cyber Security Compliance (CPCSC) – Level 1 or 2

What it is: Canada's cyber certification program.

Who needs it: Suppliers in the Canadian defence supply chain.

Levels:

Level 1: Basic cybersecurity hygiene - Basic contracts with minimal cybersecurity risk, such as suppliers providing commercial goods or services where only publicly available or low-sensitivity information is handled.

Appendix – Completing the DRP Application Form (cont'd)

- Level 2:** Protection of sensitive defence information
- Standard defence contracts where suppliers handle controlled or sensitive defence information (e.g., technical data, project documentation) requiring defined cybersecurity safeguards.
- Scope:** Policies, access control, incident response, system hardening.
- Typical use:** Required by the Department of National Defence (DND).
- Level 3:** Advanced protection of highly sensitive defence information.
- Scope:** Continuous monitoring, threat detection and response, advanced access controls, secure system architecture and enterprise-wide risk management.
- Typical use:** Required for high-risk defence contracts where protection against sophisticated cyber threats (e.g., advanced persistent threats) and highly sensitive information is critical.
- **Cybersecurity Maturity Model Certification (CMMC) – Level 1 or 2**
What it is: A U.S. Department of Defense (DoD) cybersecurity certification.
Who needs it: Companies bidding on U.S. defence contracts.
Levels:
Level 1: Basic safeguarding of Federal Contract Information (FCI).
Level 2: Protection of Controlled Unclassified Information (CUI).
Scope: Access control, audits, configuration management, incident handling.
Typical use: Mandatory for many DoD contracts.
 - **ISO 27001**
What it is: An international information security management standard.
Who needs it: Any organization wanting globally recognized information security certification.
Scope: Risk management, governance, policies, continuous improvement.

- Strength:** Broad, business wide information security framework.
- Typical use:** Technology companies, SaaS providers, global enterprises.
- **NIST 800 171**
What it is: A U.S. cybersecurity standard for protecting sensitive government data in non federal systems.
Who needs it: Contractors handling Controlled Unclassified Information (CUI).
Scope: 110 security controls across 14 control families.
Typical use: Often a baseline requirement for CMMC Level 2.
 - **Other (specify)**

Quick Comparison Snapshot

Category	Focus	Geography
Reliability Status	Individual trust check	Canada
DOS / DSC / FSC	Facility & organization security	Canada
CGP	Military-controlled goods	Canada
CPCSC	Defence cybersecurity	Canada
CMMC	Defence cybersecurity	USA
ISO 27001	Enterprise information security	Global
NIST 800 171	Government data protection	USA

C) DEFENCE MARKET INFORMATION

- Defence markets currently served (Canadian, American, other, or none).
- Markets you wish to enter, based on the work initiated under the DAIR DRP.
- Your current status in the defence industry:
 - Direct government contract.
 - Contracting through OEM.
 - Contracting through a Tier 1 supplier.
 - Diversifying (or interested) into defence.

Appendix – Completing the DRP Application Form (cont'd)

SECTION 4 – Annual Revenue

- Provide:
 - a) Applicant's annual revenue.
 - b) Applicant's export revenue.
 - c) Percentage of revenue from civil aerospace and/or defence-related aerospace for both:
 - 2025 actual.
 - 2026 forecast.

SECTION 5 – General SME Information

Provide descriptive, narrative information covering:

5a – Mission, Vision, and Values

Describe the company's purpose, direction, and guiding principles.

5b – Company Activities

Detail:

- Products manufactured (e.g., structures, gears, engine components, landing gear parts).
- Industries served.
- Materials used (e.g., metal, composites).
- Services provided (e.g., engineering, machining, metal finishing).

5c – Other Certifications

List any additional certifications such as:

- AS9100.
- NADCAP.
- ISO 14001.

5d – Past and Current Relationship with DAIR

Identify if you have previously and/or currently participated in:

- SDI.
- Green Fund.
- Innovation Network.
- DAIR To Innovate Tech Showcase.

SECTION 6 – Declaration and Signature

Authorized signatory must confirm:

- All provided information is accurate.
- Consent for DAIR to share information with a secure compliance third party.
- Disclosure of lobbyist involvement in accordance with the Lobbying Act.
- No conflicts of interest exist.
- Compliance with applicable public-sector ethics requirements.
- DAIR will be informed of major corporate or financial changes.
- Funding is only available once the assessment process is satisfactorily completed.

Signature fields required:

- Full name.
- Signature.
- Date.



DAIR

DOWNSVIEW AEROSPACE | DOWNSVIEW AÉROSPATIALE
INNOVATION & RESEARCH | INNOVATION & RECHERCHE