



# Canadian Defence Market Entry Roadmap

A PRACTICAL GUIDE FOR YORK REGION MANUFACTURERS

Published: April 2026

# EXECUTIVE SUMMARY

Canada is making substantial investments -- more than \$180 billion in procurement and \$290 billion in capital and infrastructure investment -- in its defence sector over the next decade.

These investments are being done to meet new NATO spending commitments (5% of GDP) and to grow the economic and innovative capacity of the domestic defence manufacturing sector.

Other NATO countries such as Germany and Poland and trading partners like Japan and South Korea, have committed to increased defence spending. These increases are done to meet NATO spending commitments and to be better prepared considering regional conflicts, such as the Russian-Ukrainian war.

Despite these commitments, it will be difficult for many countries to meet NATO targets in the short term. This is due to limited supply chain capacity and the pace at which governments award defence-related contracts.

Given this, it is widely anticipated that there will be substantial opportunities for York Region manufacturers to supply the defence sector in Canada and abroad.

These opportunities are likely to be realized by the best prepared and most proactive suppliers, and by companies with relevant or nascent capabilities that are ready to invest in their operations and business practices to leverage their capacity, expertise and competitive advantage.

This roadmap is designed to support manufacturers that are seeking to grow and scale their existing defence-related business, and to those that do not currently supply the defence sector but are interested in pivoting or transitioning some or all their business to defence-related activities.

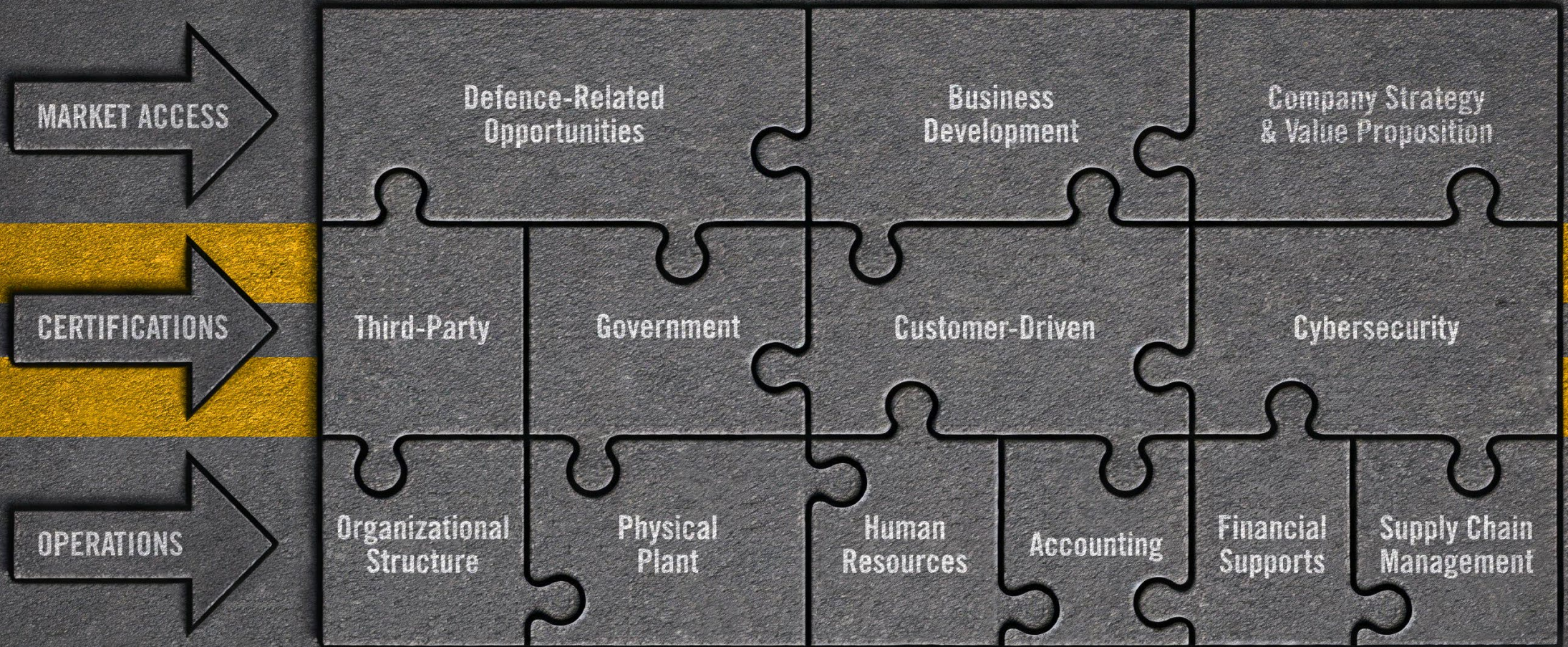
In addition to an overview of the defence sector, the roadmap provides insight into several important business practices that manufacturers aspiring to supply the defence sector will need to consider as they explore these exciting opportunities.

# CONTRIBUTOR ACKNOWLEDGEMENT

We would like to express our profound thanks to the companies, business leaders, and ecosystem partners that contributed to our Canadian Defence Market Entry Roadmap.

- Automotive Parts Manufacturers' Association (APMA)
- Canadian Manufacturers & Exporters (CME)
- Circuit Tech Inc.
- Department of National Defence
- Downsview Aerospace Innovation & Research (DAIR)
- Federal Economic Development Agency for Southern Ontario (FedDev Ontario)
- Intertek Group
- Letar Inc.
- Litens Automotive Group
- Megalab Group Inc.
- Microart Services Inc.
- Mitsubishi Heavy Industries Canada Aerospace (MHICA)
- Next Generation Manufacturing Canada (NGen)
- Ontario Aerospace Council (OAC)
- Ontario Ministry of Economic Development, Job Creation & Trade (MEDJCT)
- Ontario Vehicle Innovation Network (OVIN)
- Pfaff Technologies

# KEY ELEMENTS FOR MANUFACTURERS TO UNLOCK DEFENCE SECTOR OPPORTUNITIES



# CANADIAN DEFENCE MARKET ENTRY ROADMAP GUIDE

## Section I: The Defence Sector

- Canada's Defence Industrial Strategy ... 7
- International Defence Industrial Strategies ... 8
- Core Industry Segments ... 9
- Supply Chain Tiers ... 10
- Dual-Use Technologies ... 14

## Section II: Market Access

- Accessing Defence-Related Opportunities ... 16
  - Procurement
  - Industrial & Technological Benefits (ITB)
- Business Development ... 17
  - Incumbent Defence Manufacturers
  - Aspiring Defence Manufacturers
- Company Strategy & Value Proposition ... 18

## Section III: Certifications

- Overview ... 20
- Third-Party ... 21
- Government ... 22
- Customer-Driven ... 23
- Cybersecurity ... 24
- Timelines & Cost ... 25

## Section IV: Operations

- Organizational Structure ... 27
- Physical Plant ... 28
- Human Resources ... 29
- Accounting ... 30
- Financial Supports ... 31
- Supply Chain Management ... 32



SECTION I

**THE DEFENCE SECTOR**

# DEFENCE INDUSTRIAL STRATEGY (DIS)

## A Canadian Priority

### Geo-Political

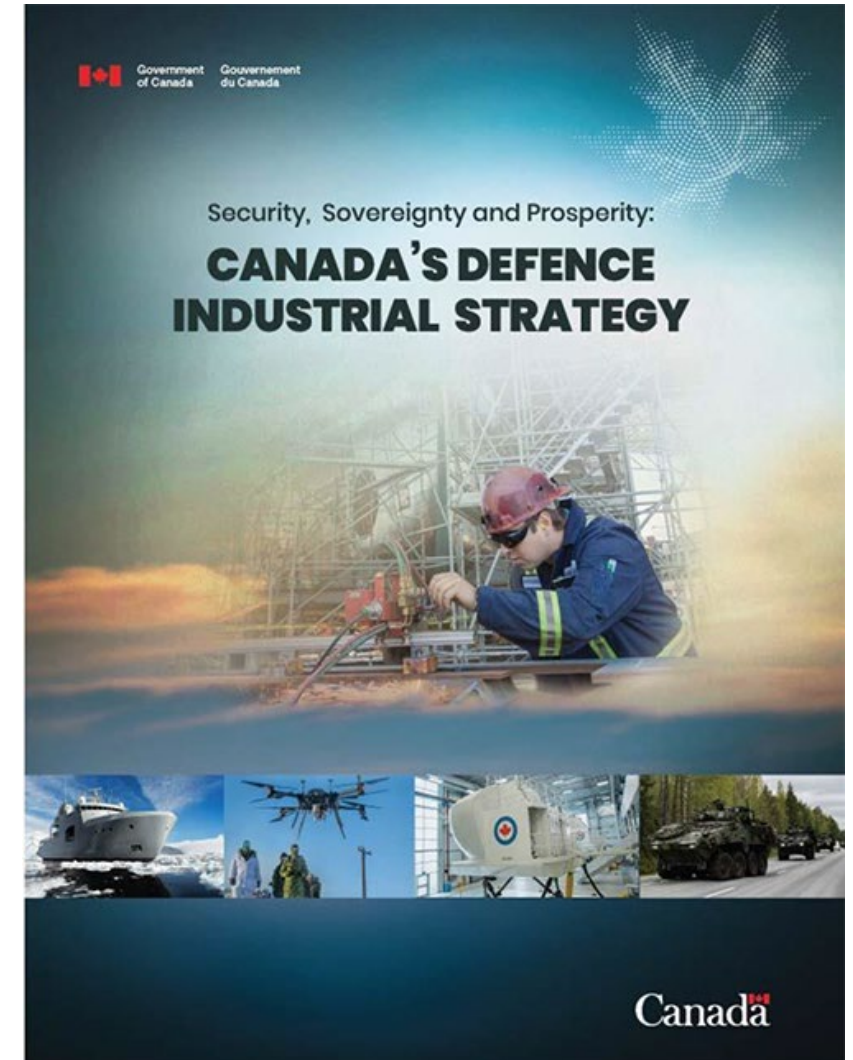
- International alliances and trade relationships depend on Canada's ability to defend itself from hostile actors and contribute to multi-national defence initiatives

### National Security & Sovereignty

- Ongoing and potential conflicts threaten geo-political stability and the sovereignty of allies and trading partners, as well as international supply chains

### Economic

- Canada's DIS is a means to increase manufacturing output, foster innovation, create opportunities, and maintain employment, especially for businesses and workers displaced from other industries (e.g. automotive)

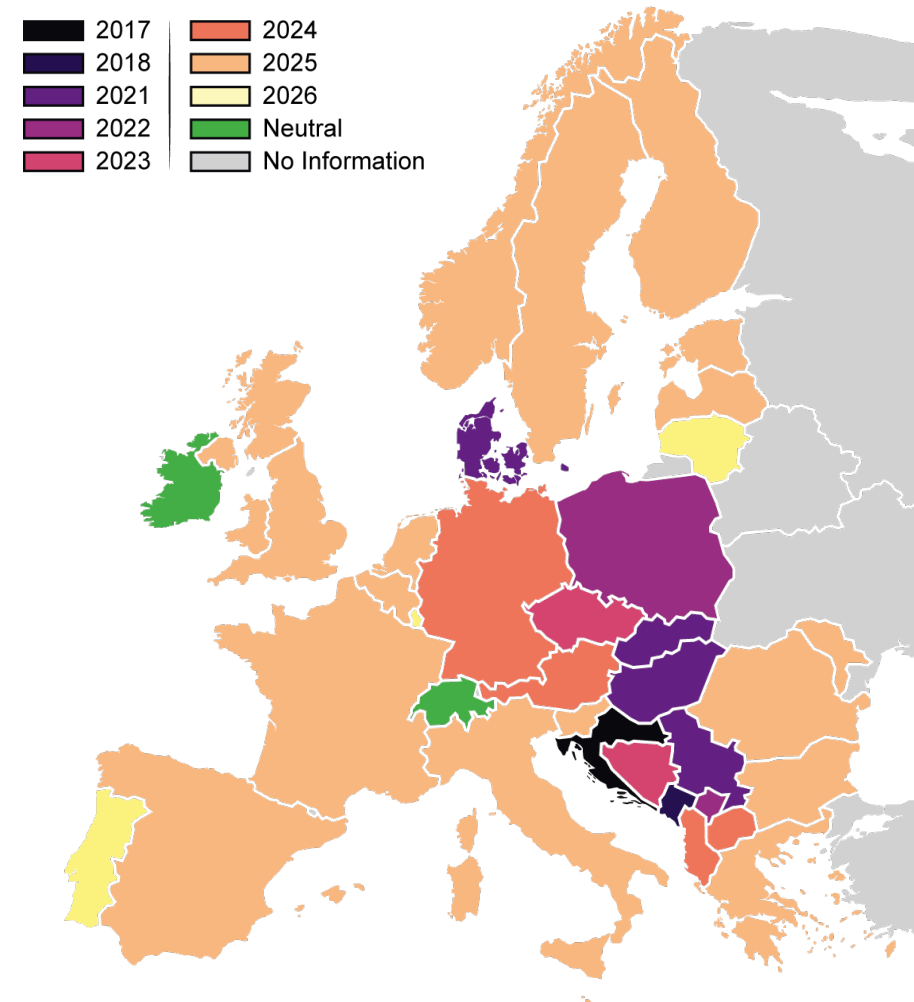


# DEFENCE INDUSTRIAL STRATEGY

## Not just a Canadian Priority

- Defence is a priority for the United States, Germany, Japan, South Korea, and other allies and global trading partners
- The United States invests in defence as part of its broader industrial strategy, with the 'Big 5' contractors -- Boeing, General Dynamics, Lockheed Martin, Northrop Grumman, and RTX -- playing a major role in its economy
- European countries have implemented and updated defence strategies in response to the Russian-Ukrainian war, with domestic companies (e.g. Rheinmetall, Airbus, Saab, Thales), US-based, and South Korea-based manufacturers playing an important role
- Japan and South Korea have implemented new strategies and increased defence spending to deter threats to Taiwan's sovereignty and foster closer ties with key trading partners including the United States

Recent European National Defence Strategies by Year



# CORE INDUSTRY SEGMENTS



**LAND SYSTEMS**



**AIRCRAFT**



**SPACE**



**MARINE**



**ORDNANCE**



**C4ISR**

# SUPPLY CHAIN TIERS

## Original Equipment Manufacturers (OEMs) & Prime Contractors

Lead contractors responsible for full system delivery (integration, project management, assembly of ships, aircraft, combat vehicles etc.)

## TIER I: Major Subcontractors & Subsystems

Critical, complex modules and subsystems supplied to OEMs and Primes (*center fuselage, engines, landing gear, radar, etc.*)

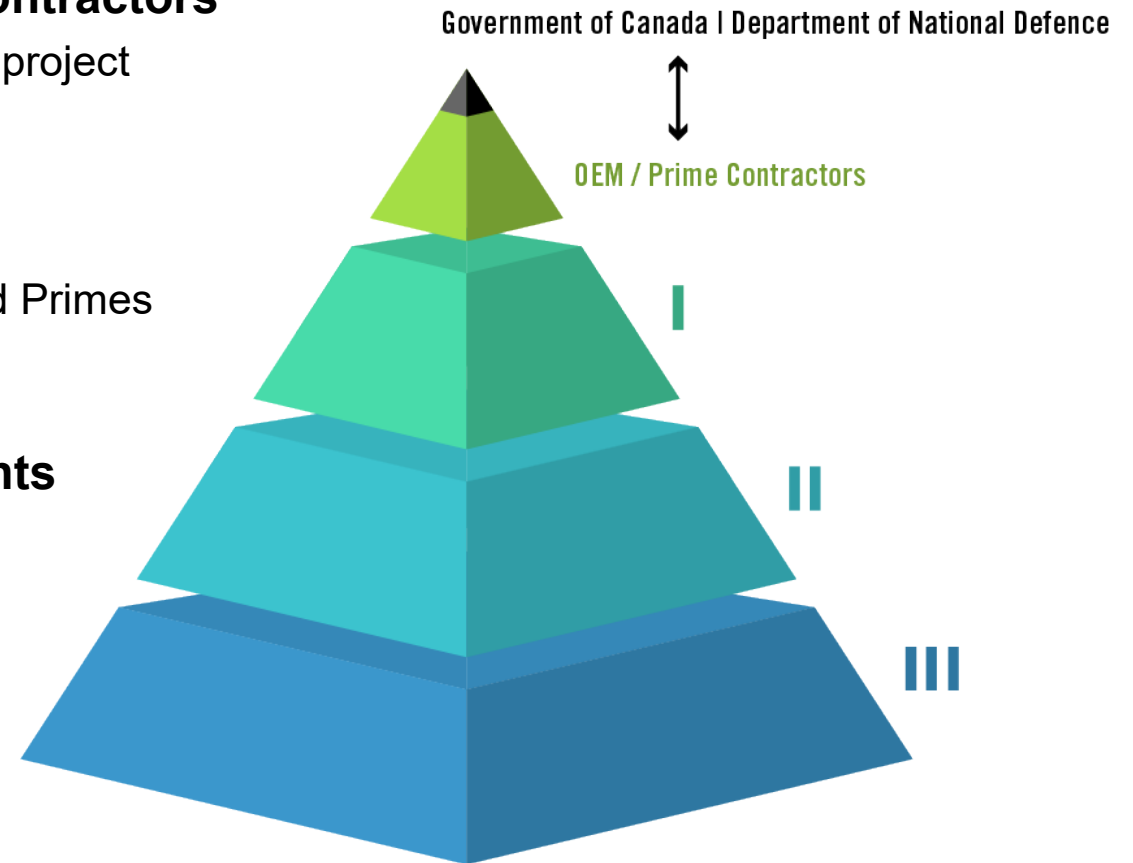
## TIER II: Specialized Manufacturers, Parts & Components

Parts, modules, and technical components supplied to Tier 1 (*machined parts, circuit boards, software modules, etc.*)

## Tier III (and lower): Raw Material & Basic Components

Basic materials and parts (*metals, composites, specialized electronics, etc.*)

There are several important distinctions when compared to the automotive industry. In the automotive sector, an OEM such as Toyota or Volkswagen is the end customer, broadly equivalent to a defence OEM or prime contractor. In defence, however, the customer or sponsor is the ultimate recipient or end user, such as the RCAF or the U.S. Navy, rather than the prime contractor itself. As a result, virtually all work is custom, highly controlled, and confidential, and is produced to exact, program-specific requirements rather than standardized commercial specifications..



# ORIGINAL EQUIPMENT MANUFACTURERS & PRIME CONTRACTORS

These are the primary recipient of government-sponsored defence contracts. They are responsible for project management, engineering, integration, production, and delivery of aircraft, ships, vehicles, satellites, armaments, and other complete defence systems.

Prime contractors have extensive experience in the defence sector and tend to be very large companies.

The market capitalization\* of many prime contractors (primes) is substantial, for example:

- RTX | **\$284 Billion**
- Lockheed Martin | **\$155 Billion**
- General Dynamics | **\$97 Billion**



The market capitalization\* of prime contractors is considerably larger than Canada's largest manufacturers, such as:

- Bombardier | \$18 Billion
- Magna | \$16 Billion
- Linamar | \$5 Billion
- BRP | \$5 Billion

## Key Canadian prime contractors:

- Irving Group | Ship Building
- MDA Space | Satellites & Robotics
- CAE | Training Simulators
- Bombardier | Aircraft

\* Market Capitalization figures are all \$USD

## TIER I | CRITICAL MODULES & SYSTEMS

Tier I defence suppliers are responsible for delivering critical and complex modules, systems and sub-systems (e.g. center fuselage, landing gear, engines, communications equipment) to OEMs and prime contractors (primes).

Most OEMs and primes are also involved in Tier I activities. For example, RTX-owned companies such as Pratt & Whitney and Collins Aerospace are important Tier I suppliers to aircraft OEMs.

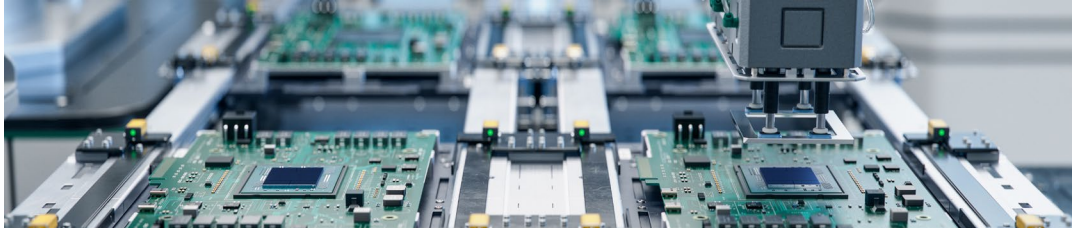
Some small and medium-sized enterprises (SMEs) operate as Tier I suppliers. However, many Tier I defence suppliers are very large and well-known companies including L3Harris, Rolls-Royce, and GE Aviation.

In some cases, Tier I suppliers have a larger market capitalization than the OEM and prime contractors that they supply.

Most major defence contracts engage several large defence contractors. As such, OEMs and Tier I defence suppliers simultaneously compete for and collaborate on major defence contracts.



# TIERS II & III | SPECIALIZED PARTS & BASIC COMPONENTS



## Tier II

Tier II suppliers produce specialized components, parts, and modules for OEMs, primes, and Tier I companies. This includes machined and manufactured components, electronic modules, printed circuit boards, and welded assemblies. A majority are SMEs.

A large majority of Canada's more than 1,000 defence manufacturers are best categorized as Tier II suppliers. Most manufacturers that pivot or transition into the defence sector will be Tier II companies.

Making the jump from Tier II to Tier I requires significant investment and scaling. It is unclear at this point whether supporting this transition is a targeted goal of Canada's Defence Industrial Strategy.



## Tier III (and lower)

Tier III suppliers produce raw materials and basic components (e.g. steel, rubber, metal powders, electrical components) for higher tier manufacturers.

These manufacturers may carry out valuable and specialized work, but they are often not immediately recognizable as defence manufacturers. Most supply several industries.

As part of the defence supply chain, Tier III suppliers must undergo rigorous certification and accreditation processes, like OEMs and Tier I/II suppliers.

# DUAL-USE TECHNOLOGIES



Dual-use technologies include products with both civilian and military applications. The current working definition of 'dual use' within the federal government is broad. It may differ from more technical definitions preferred by the defence sector.

This broad and expansive definition is purposeful. It offers flexibility to help reach NATO spending targets and to facilitate the inclusion of companies that are not traditionally part of the defence sector supply chain. The definition of 'dual use' may become more refined over time.

Examples of dual-use technologies or products include:

- Bombardier Global 6500 aircraft (and components thereof) that can be outfit for business or for military intelligence, surveillance and reconnaissance (ISR) purposes;
- Highway, port, and telecommunications infrastructure that serve military installations and civilian communities;
- Low-earth orbit (LEO) satellites (and components thereof) made by MDA that are primarily used for civilian applications, but that can be modified for mission-critical military ISR purposes; or
- Flight training simulators designed and manufactured by CAE that are to train civilian and air force pilots

While the term 'dual-use' refers to products that have civilian and defence applications, we use the term 'diversified' to refer to a company that serves customers in multiple sectors including defence.



## SECTION II

# MARKET ACCESS

---

Companies considering a pivot or transition into the defence sector need to understand where to find market opportunities and how to develop their business to leverage those opportunities. This section looks at the broader business processes required to enter the defence market.

# ACCESSING DEFENCE-RELATED OPPORTUNITIES

## Procurement

Canadian public security clearance defence contracts are advertised online. The Department of National Defence (DND) [Defence Capabilities Blueprint](#) provides an overview of projects, status, timelines, and the Defence Capability Investment Areas involved.

Public Sector Procurement Canada's (PSPC) [Canada Buys](#) features a range of contracts tendered by the federal government, including departments, DND and the Canadian Coast Guard (CCG).

Contracts tendered on federal websites tend to be large in scope and accessible primarily to OEMs/Primes or Tier I suppliers. However, they can help Tier II and Tier III suppliers understand the scope, nature, and timeline of defence contracts.

The [Defence Investment Agency](#) is mandated to streamline and modernize procurement activities, and to serve as a single interface across multiple departments.

## Industrial & Technological Benefits (ITB)

Canada's ITB policy requires that companies awarded major defence procurement contracts engage in business activity equal to the value of those contracts, and to conduct a prescribed proportion of that work in the country with Canada-based SMEs.

ITBs are administered by Innovation, Science and Economic Development Canada (ISED), but Federal Regional Development Agencies such as FedDev Ontario play an important role in connecting SMEs (e.g. Tier II suppliers) with OEMs/Primes and Tier I suppliers and ITB-related opportunities.

More information about ITBs, and contact information for FedDev Ontario, is available [here](#).

# BUSINESS DEVELOPMENT

## Incumbent Defence Manufacturers

Incumbent defence manufacturers often leverage well-established networks, including customers and partners, to learn about opportunities. In addition to customers, they work with industry associations, attend trade shows, and engage with government agencies (e.g. [FedDev Ontario](#)) to build relationships within those networks.

These relationships are underpinned by:

- Technical capabilities;
- Reputation;
- A well articulated company strategy and value proposition

Trade shows and industry events are first and foremost opportunities to connect with existing customers and partners.

## Aspiring Defence Manufacturers

Aspiring defence manufacturers may approach business development differently than incumbents.

Connecting with customers that may be incumbent defence sector suppliers to understand their needs, and the potential for the aspiring defence manufacturer to meet those needs, is an important initial step.

A functional website that is refreshed and updated regularly (every two years is recommended), an up-to-date company LinkedIn page, and profiles of key personnel is advisable. These will be the point of entry for many potential customers and partners. Certifications such as ISO 9001 should be featured prominently.

Attending trade shows and industry events is important. Risk-averse Tier I and Tier II defence contractors value familiarity and are more likely to engage with companies and people that invest in relationship-building.

# COMPANY STRATEGY & VALUE PROPOSITION

Developing and articulating a company strategy and value proposition is an important part of defence sector business development.

Understanding how Canada's Defence Industrial Strategy and broader opportunities in the defence sector align with company strategy and value proposition is an important part of defence-related business development. A well-developed company strategy and value proposition -- including mission, vision, and values -- demonstrates sophistication and thoughtfulness.

The ability to communicate how company strategy and value proposition aligns with defence sector opportunities can be a valuable part of initial conversations with potential customers and partners. One potentially useful step is to identify which of the [17 Key Industrial Capabilities](#) (KIC) listed within the DND Defence Capabilities Blueprint are core company capabilities.

[BDC](#) offers useful resources for companies seeking to develop or update their strategic plan and value proposition.





## SECTION III **CERTIFICATIONS**

---

Certifications are an efficient and accepted way to communicate a company's level of sophistication, capabilities, and potential to develop additional capabilities to prospective customers and partners

# OVERVIEW

The defence sector relies on interconnected systems, modules, and components that operate flawlessly in rugged environments. It is at best impractical and at worst impossible to replace or modify faulty components within equipment that is operating high in the air, in space, or beneath the surface of the ocean. As such, developing, manufacturing, testing, and accrediting defence-related products and technologies is subject to stringent regulations, process certifications, and audits.

These certifications and audits are necessary to do business in the defence sector. The processes, timelines, and costs associated may seem onerous, but are important to overall company strategy. An active and persistent approach when engaging with certification organizations and auditors is often necessary to expedite timelines. A passive approach such as sending an email and hoping for a reply, will lead to delays and frustration.

The following pages will address what types of certifications and audits may be required to enter the defence sector as a supplier.



# THIRD-PARTY QMS CERTIFICATIONS

International Standards Organization (ISO) quality management systems (QMS) certification is generally considered to be the bare minimum for companies interested in supplying the defence sector.

ISO certifications follow international-industry based standards and tend to emphasize proper documentation and record-keeping, where other programs such as Nadcap place more emphasis on shop floor processes.

Aspiring defence manufacturers that are not ISO certified should start with **ISO 9001 certification**. This focuses on QMS including processes, continuous improvement, and risk management. After ISO 9001 certification, organizations should look at other certifications including:

- **AS9100** (aerospace, space, & defence)
- **IATF 16949** (automotive)
- **ISO 13485** (medical devices)
- **ISO 14001** (environmental)
- **ISO 45001** (OH&S)
- **ISO 27001** (cybersecurity)
- **ISO 17025** (testing & calibration)

Companies must engage a third-party auditor such as Intertek, Bureau Veritas, and others to manage the certification process. ISO certifications must be maintained and updated over time.

This includes audits every one to three years. The initial cost depends on company size and complexity. Subsequent audits tend to be less costly than the initial certification process, especially when companies keep meticulous records.

Auditors can help companies stay up-to-date regarding changes to ISO standards and offer valuable insight to support process improvements.



# GOVERNMENT CERTIFICATIONS (CGP & ITAR)

Federal legislation requires that companies register in the Controlled Goods Program (CGP) to access, handle, or transfer military goods and goods of national security significance. International Traffic in Arms Regulations (ITAR) govern the control, sale, and export of defence-related goods and technologies in the United States.

CGP and ITAR are largely harmonized to facilitate trade and integration between Canada and the United States. The jointly-administered Joint Certification Program (JCP) facilitates shared access of technical data between CGP-registered companies in Canada and ITAR-compliant companies in the United States.

There is no direct cost to register in the CGP, but there are indirect costs. These are mostly associated with staff time associated with the registration process and subsequent maintenance work, or with hiring a consultant to support CGP registration. There may be additional costs associated with operational improvements, which are examined in Section IV.

CGP and ITAR are designed with security in mind, rather than QMS. Companies tend to have personnel dedicated to CGP compliance activities. Subcontractors (e.g. trades, janitorial, security, employment agencies) may also need to be CGP-registered if they will encounter defence-related goods or processes as part of their work.

More information on [registering in the CGP is available](#). Processing times are significantly longer than normal due to a surge in applications and renewals as of March 2026.

In some cases, additional government clearances and security assessments including those conducted by CSIS, may be required for key personnel working on classified or secret projects. These types of assessments evaluate national loyalty and reliability through detailed background checks.

# CUSTOMER-DRIVEN CERTIFICATIONS

Customer-driven OEMs/Primes and Tier I defence contractors have internal auditors that work closely with Tier II and Tier III suppliers. Customers may have requirements in addition to those included in ISO 9001, AS9100, or other third-party certifications. These may relate to end use, process controls, security, or documentation.

OEMs/Primes and Tier I defence contractors make a significant investment when they choose a supplier. Their internal auditors are there to support the supplier, while also protecting the interests of their employer. Customer auditors must be treated with the utmost respect.

One example of a customer driven technical requirement is MIL-Spec, a United States Department of War (DOW), formerly the Department of Defense, standard that defines reliability, durability, and interchangeability for military products.

In Canada, it is not a default requirement, but contract specific standards under the Defence Production Act may call for Canadian, NATO, or U.S. MIL-Spec when interoperability is needed. MIL-Spec is typically used when integrating with U.S. or NATO systems, using military off the shelf products, or when specified by the technical authority.

Compliance involves meeting DOW standards and completing tests such as MIL-STD-810 or MIL-STD-461 through accredited labs, with documentation submitted for Qualified Products List eligibility.

Defence projects may also require other military or civilian standards, including those for interoperability with allies or commercial standards like CE and UL for dual-use technologies.

# CYBERSECURITY CERTIFICATIONS

Canadian and U.S. cybersecurity certification programs are designed to help non-government organizations protect sensitive and classified information.

## **Cybersecurity Maturity Model Certification (CMMC):**

Required to work on contracts within the United States DOW and includes manufacturers in Canada that export to the United States. The CMMC is a multi-tiered program. Requirements for an individual company depend on the product being manufactured. The CMMC closely follows guidelines established by the National Institution of Standards and Technology of the United States (NIST).

## **Canadian Program for Cyber Security Certification (CPCSC):**

A requirement for Canadian defence contracts. The first phase of the CPCSC was rolled out in 2025, with a full rollout expected in 2026. The CPCSC also follows NIST guidelines.

Both CMMC and CPCSC require third-party auditors. Certification can take a year or more, and cost more than \$100,000. This cost does not include potential upgrades to software and IT infrastructure. There are also monthly costs associated with maintaining CMMC and CPCSC certification.



# TIMELINES & COSTS

Type	Timeline	Direct Costs	Indirect Costs
ISO	6-18 Months	Yes	Possible
CGP	3-18 Months	No	Possible
Customer-driven	3-6 Months	Yes	Possible
Cybersecurity	6-18 Months	Yes	Yes

Indirect costs may include but are not limited to: time spent documenting existing processes; upgrades to physical plant such as security devices and entranceways, IT infrastructure, software; and staff training. Some costs are both one off and ongoing such as recertification audits, IT upgrades etc.

Dollar cost estimates are not provided as numerous factors can significantly affect cost variability between companies.



# SECTION IV OPERATIONS

---

There are several important and unique operational considerations that defence manufacturers should be aware of and apply to both incumbent and aspiring defence sector manufacturers. This section looks at what those key operational considerations are.

# ORGANIZATIONAL STRUCTURE



The operational and regulatory requirements associated with defence sector work are considerably different than those associated with most other industries. In addition to certifications and audits, these requirements extend to the physical plant, human resources, accounting and finance, and supply chain management.

As a company's defence sector work grows in scope, scale, and complexity, it may be necessary to reconsider how the company is organized, and to separate defence-related activities from other activities.

For example, it may be impractical to have every employee of a medium-sized company receive security clearance if only 10% of revenue comes from defence-related work.

In such cases, companies (especially smaller ones) may consider establishing a small team and/or area of the plant that focuses primarily or exclusively on defence-related work. In others, companies may consider a separate division, including an additional or separate facility that focuses exclusively on defence-related work.

It is therefore important to continuously assess how the operational and regulatory requirements of defence-related work (and the associated costs) affect the company's overall strategy and organization.

# PHYSICAL PLANT

Incumbent and aspiring defence manufacturers may be required to make upgrades to their physical plant, building, factory or property. These upgrades are often directly related to the security requirements associated with defence sector work.

## Upgrades may include:

- Secure, two-stage, or 'airlocked' entry points and reception zones
- Electronic access for employees and subcontractors (fingerprint or facial recognition)
- Detailed visitor logs
- Secure fencing around exterior entry points, the building, or property
- Alarm systems including motion detectors
- Defence-related production activities may need to be sequestered from other activities. This may involve individual machine(s), office, room, or section of the plant. In some cases, it may involve 'masking' key product or process information from employees.



# HUMAN RESOURCES

There are several human resource management practices that are relevant to defence sector manufacturers. These include background checks and security clearances for employees and dedicated roles for key personnel.

## Background Checks

CGP registration requires criminal background checks for employees. These background checks are similar in nature to the background checks required of persons who volunteer with youth or community groups. These checks are less focused on petty crimes from the distant past and more focused on criminal activity that undermines loyalty and reliability, such as fraud.

More advanced background checks may be required in some instances and may probe an applicant's relationship with persons or organizations from hostile countries.

Employers can expect to learn unexpected things about their employees through this process. It may be advisable to integrate basic background checks into hiring and recruitment practices.

## Dedicated Defence Sector Personnel

It may be useful to dedicate personnel to defence-related activities as that proportion of a company's business grows.

This may include an executive or management lead, such as a company owner or part-owner, sales and business development personnel, engineering and production leads, and CGP and/or ITB leads, who are responsible for interfacing with federal government agencies. Individual employees may take on more than one of these roles, where applicable.

This practice assures that proper attention and focus is paid on defence-related business activities without interrupting other civilian-related business activities.

# ACCOUNTING

Defence contracts often operate on a 'cost-plus' basis, whereby the customer or sponsor reimburses the supplier for allowable expenses (e.g. material, labour, overhead), plus a pre-negotiated profit margin, and/or bonus payments.

Cost-plus contracts require that suppliers share financial information with customers or sponsors and adhere to detailed accounting practices.

These practices may involve maintaining strict records of employee working time and activities. Such practices have very little tolerance for 'freewheeling', forgetful, and/or wayward employees.

Defence contracts, especially those that involve government agencies directly, may also require more rigorous financial audits. Consult your audit and accounting services provider(s) in the early stages of pursuing opportunities in the defence sector.



# FINANCIAL SUPPORTS

Traditional financial institutions have historically been hesitant to finance defence manufacturing investments. Government programs have emerged to fill this gap.

[Business Development Bank of Canada \(BDC\)](#): a Crown Corporation mandated to support Canadian businesses. It recently introduced a [Defence Platform](#), which will deploy up to \$4B to support Canadian defence sector SMEs. This includes \$500M in the StrongNorth venture capital fund designed to accelerate innovation and growth among early-stage companies.

[Export Development Canada \(EDC\)](#): a Crown Corporation mandated to support and develop trade between Canada and its trading partners. EDC has broadened its approach to financing and insurance-related support for export-oriented defence manufacturers. In 2025, EDC provided more than \$690M in commercial support to 28 Canadian defence companies.

[Regional Defence Investment Initiative \(RDII\)](#) – Supported locally through FedDev Ontario and is offering nearly \$200M to support businesses seeking to enter or grow within the defence sector. Funding is offered as a repayable contribution.



# SUPPLY CHAIN MANAGEMENT

With few exceptions, defence manufacturers at all supply chain tiers must source materials, components, and other inputs from accredited and certified suppliers. Customers, government agencies, and/or certification bodies may play a role in identifying these suppliers, and in auditing supply chains on a periodic or ongoing basis.

Sourcing materials, components, or inputs from non-accredited or uncertified suppliers may lead to the product being rejected by the customer or sponsor, with the offending company responsible for the costs of those materials, components, or other inputs.

There are a limited number of companies that can supply certain accredited, defence-grade materials and components. As defence spending increases, many of these accredited suppliers will face order backlogs due to high demand. 'Dynamic' trade and tariff regulations can also affect pricing and availability.

It is important that incumbent and aspiring defence sector manufacturers understand the landscape of defence-accredited suppliers, tariffs (and potential tariffs), and the associated timelines (and delays) to procure materials and components. All of these should be factored into cost analysis and bids.

A key membership to support sound supply chain management, is the [Government-Industry Data Exchange Program \(GIDEP\)](#). This is a US-Canadian cooperative, no-cost program to share technical information, reducing, or eliminating, duplicate expenditures of resources.

By participating, companies can avoid using faulty, counterfeit, or obsolete parts, thereby saving billions in potential rework and ensuring the reliability of military systems. It is often a contractual requirement for defense contracts, especially those exceeding \$500,000.



IN  
**SUMMARY**

## OPPORTUNITY EXISTS, BUT PLANNING AND A WILLINGNESS TO INVEST ARE CRUCIAL FACTORS

There are ample domestic and export-oriented opportunities ahead for incumbent and aspiring defence manufacturers. To realize these opportunities companies must be prepared to make medium-term investments in several aspects of their business.

This roadmap outlined how companies can identify defence sector opportunities and build a strategy and value proposition to position themselves advantageously to prospective customers and partners. It demonstrates the importance of certifications and audits and several operational considerations that defence suppliers should be aware of.

Finally, it identifies several government supports, industry associations and innovation partners, and industry events that can help companies grow and scale their existing defence business or transition some or all their business into the defence sector.



# KEY INDUSTRY ASSOCIATIONS & INNOVATION PARTNERS

## Industry Associations

- Aerospace Industries Association of Canada (AIAC)
- Alliance of Canadian Defence Companies (ACDC)
- Canadian Association of Defence and Security Industries (CADSI)
- Canadian Manufacturers and Exporters (CME)
- Ontario Aerospace Council (OAC)
- Ontario Defence Association (ODA)

---

## Innovation Partners

- Academic Institutions
- Downsview Aerospace Innovation & Research (DAIR)
- Next Generation Manufacturing Canada (NGen)
- Ontario Centre of Innovation (OCI)
- Ontario Regional Innovation Centres (RICs)
- Ontario Vehicle Innovation Network (OVIN)



# IMPORTANT DOMESTIC INDUSTRY EVENTS

- DEFSEC West | Calgary
- NGen N3 Summit | Toronto
- CANSEC | Ottawa
- Best Defence | London
- DAIR to Innovate | Toronto
- DEFSEC Atlantic | Halifax
- CME National Manufacturing Conference | Ottawa



Photo Credit: Canadian Association of Defence and Security Industries

For additional information:

**York Region Economic Development**

[www.yorklink.ca](http://www.yorklink.ca) | [edo@york.ca](mailto:edo@york.ca)

---

