POLICY-ALIGNED RECOMMENDATIONS TO MODERNIZE CANADA'S DEFENCE INTELLECTUAL PROPERTY FRAMEWORKS

Strengthening Ottawa's Defence Small and Medium-Sized Enterprise Ecosystem

FROM: STRATFORD INTELLECTUAL PROPERTY DATE: MAY 27, 2026

Is Canada's defence procurement system helping innovators scale, or making it harder to protect what they build?

Canada's defence sector is entering a critical moment. As the federal government modernizes defence procurement and intellectual property frameworks, many Canadian innovators are facing growing concerns around how their technologies, data, and intellectual property will be protected, commercialized, and scaled.

This report captures insights from a 2026 defence industry roundtable held in Ottawa with representatives from across Canada's defence ecosystem — including SMEs, technology innovators, and established defence organizations. The discussions revealed a shared concern: while Canada depends on homegrown innovation to strengthen national security and meet NATO and Five Eyes commitments, current procurement and contracting practices may unintentionally limit the growth and global competitiveness of Canadian firms.

From cybersecurity and AI to autonomous systems and digital infrastructure, Canadian companies are developing technologies critical to sovereign capability. This report explores the barriers these organizations face and outlines practical recommendations to better support innovation, commercialization, and long-term defence readiness.

PREPARED BY PAUL FORTIN, NATALIE GIROUX AND MYRIAM DAVIDSON OF STRATFORD INTELLECTUAL PROPERTY

ALIGNED WITH THE GOVERNMENT OF CANADA DEFENCE POLICY UPDATE AND FEDERAL BUDGET PRIORITIES

AT A GLANCE

Executive Summary

This report was prepared based on a defence industry roundtable convened in the fall of 2026 at Invest Ottawa, which brought together a broad cross-section of Canada's defence industrial base. Participants included small and medium-sized defence enterprises as well as larger original equipment manufacturers (OEMs), all of whom provided candid, practitioner-level feedback.

The discussions focused on shared concerns and practical challenges arising from the Government of Canada's proposed and anticipated recommendations to modernize Canada's defence intellectual property frameworks. The insights captured in this report reflect real-world industry experience and are intended to inform policy development in a manner that strengthens innovation, protects sovereign capabilities, and supports the long-term competitiveness of Canada's defence sector.

Ottawa is Canada's defence innovation capital, hosting the Department of National Defence (DND), Public Services and Procurement Canada (PSPC), Innovation, Science and Economic Development Canada (ISED), North Atlantic Treaty Organization (NATO) and allied missions, and a dense cluster of defence and dual-use SMEs. These firms generate sovereign intellectual property (IP) across cybersecurity, space, command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR), artificial intelligence (AI), autonomy, and digital infrastructure that are central to Canada's NATO and Five Eyes obligations. However, government contracting templates and market structures expose SME background IP, weaken valuation through prime-contractor reach-through, stall prototype-to-commercialization transitions, and constrain exportability via the United States International Traffic in Arms Regulations (ITAR).

It is recommended to modernize defence procurement, and innovation frameworks through a set of policy recommendations and ecosystem measures that:

1. Provide default contracts to SME-safe IP positions,
2. Convert "first customer" pilots into scalable demand,
3. Codify SME IP carve-outs,
4. Anchor IP domestically via a defence patent box,
5. Raise IP literacy with government decision makers and entrepreneurs,
6. Fund IP/cybersecurity governance,
7. Professionalize prime–SME partnering, and
8. Create a Defence IP & Commercialization Hub in Ottawa.

The outcomes of this report would include increased Canadian Armed Forces (CAF) readiness; higher SME survival, faster path to commercialization, increased valuation and exports; improved return on taxpayer-funded innovation; and strengthened technology sovereignty.

Strategic Context and Problem Definition

Canada's updated defence strategy—which prioritizes increased spending, stronger NATO interoperability, and enhanced protection of critical technologies—relies fundamentally on the nation's ability to drive domestic innovation. Current procurement and IP ownership clauses are optimized for large prime contractors, not the knowledge-asset, software-first SMEs that now produce core defence capabilities. The result is IP leakage, slow transition to CAF fleet adoption[1] and reduced export competitiveness.

Contextual realities in Ottawa

- **IP-rich, asset-light firms.** SME value resides in intangible software, algorithms, data architectures, and systems knowledge. The risk of over-broad Crown licence claims or prime reach-through is therefore existential.
- **Alignment pressures.** Canada must interoperate with NATO and Five Eyes while avoiding ITAR contamination that forecloses third-market sales and depresses firm valuation.
- **Prototype dead-ends.** Innovation programs validate technology but rarely bridge to fleet adoption or export possibilities.

Objectives and Policy Principles

The key objectives are to protect and retain Canadian-controlled intellectual property, accelerate the transition from prototype development to fleet adoption, enhance the bargaining position and capital access of SMEs, drive Canadian investment by multinational OEMs, improve export readiness by avoiding unnecessary ITAR (International Traffic in Arms Regulations) entanglement, and ensure the efficient and accountable use of public funds.

Principles:

- **SME-safe by default:** Background IP remains with the SME while Crown access is purpose-bound and proportionate.
- **Mission-driven transition:** Programs measured by adoption, not pilots.
- **Sovereign where it matters:** ITAR-avoidance pathways and secure development by design.
- **Trust-based supply chains:** Fair partnering norms enforced through incentives and disclosure.
- **Fostering integration:** Promote effective collaboration and integration between technologies developed by SMEs and OEMs

[1] *Fleet adoption refers to the process by which the Canadian Armed Forces or another defence organization moves beyond the prototype or pilot phase and fully integrates new technologies or systems into its operational fleet. This means the technology is not just tested in limited circumstances but is actively deployed, maintained, and used across the relevant units or divisions. In the context of Canadian defence innovation, accelerating fleet adoption is about ensuring that innovations developed by Canadian firms—especially IP-rich, asset-light SMEs—are efficiently and widely implemented within the CAF, rather than getting stuck in prolonged testing or pilot programs.*

Expanded Analysis of Key Issues

GOVERNMENT CONTRACTING AND IP RISK

Standard Acquisition Clauses and Conditions (SACC) can expand Crown rights beyond operational necessity and expose SME background IP. Risk is amplified when deliverables blend foreground and background innovation code, data models, and toolchains.

What needs to change:

- **Mandatory Background-IP Exclusion Schedules.** Every contract includes a schedule listing background code, datasets, models, and tools—referenced by hash or repo tag—to which only limited, purpose-bound licences apply. Foreground IP ownership should also be given to SMEs (or at least license to the foreground IP).
- **"Crown Purpose Only" Licence Tiers.** Define minimum viable rights (use, reproduce, modify) solely for CAF operations and support, with no sublicensing to third parties absent compensation and SME consent.
- **IP Risk Assessment in Procurement Plans.** Require an IP impact section at bid stage (what IP is at risk, what rights are sought, mitigation).

PRIME-CONTRACTOR POWER IMBALANCES

In practice, when prime contractors hold disproportionate negotiating power, they can impose terms that allow them to access and control intellectual property created by smaller suppliers well beyond the scope of the original contract.

This reach-through not only includes the foreground IP developed for the project, but also the existing background IP that SMEs have previously invested in and rely on for their competitive advantage. Mandatory grant-back clauses may require SMEs to license their background IP to the prime or the Crown, often without additional compensation or meaningful limits on use.

Furthermore, when solutions are integrated into proprietary platforms controlled by the prime contractor, SMEs may find themselves locked out of future opportunities, as the platform owner can effectively dictate exclusivity—limiting the SME's ability to market their innovations elsewhere or participate in subsequent contracts. These dynamics can stifle innovation, reduce fair competition, reduce access to funding, reduce company value and discourage SMEs from participating in government procurement unless transparent and equitable IP protection mechanisms are enforced.

What needs to change:

- **Fair-IP Conduct Code.** Primes certify no reach-through into background and foreground IP; deviations disclosed and scored in evaluation.
- **Neutral IP Arbitration.** Rapid, low-cost binding arbitration on clause disputes to avoid time-to-cash delays.
- **Industrial and Technological Benefits (ITB) Linkage.** ITB multipliers awarded for documented SME IP protection and co-investment (not acquisition).

INNOVATION PROGRAMS THAT DO NOT SCALE

SMEs cycle through pilots and demonstrations without production contracts or export references. This pattern is common in many innovation programs, where SMEs are selected to showcase their solutions in pilot or demonstration phases, often with initial funding and support. However, despite successful technical demonstrations, these projects rarely transition into large-scale adoption or procurement by government or industry.

As a result, SMEs struggle to secure follow-on production contracts, which are critical for business growth and sustainability. Moreover, without tangible export references—evidence that their innovations have been adopted and scaled—SMEs are challenged to access new markets abroad or attract private investment. This recurring cycle of demonstration without adoption limits the impact of innovation programs, discourages SME participation, and ultimately slows the pace of technological advancement.

The implementation of a Federal patent box[2], to reduce taxes on sales of innovative products would also provide a significant incentive for companies to invest in R&D and focus on innovation.

What needs to change:

- **Automatic Phase II/III Bridges.** Clear performance gates that trigger option years and scale-up budgets.
- **Named CAF Operational Sponsors.** Each project has a unit-level sponsor with accountability for transition planning.
- **Sole-Source Conversions.** Where justified, innovation contracts can convert to time-limited sole-source production to bridge the "valley of death."
- **Defence Patent Box Options.** ISED and Finance produce design options modelled on Quebec's regime for fall fiscal update.

EXPORT CONTROLS AND ITAR CONTAMINATION

ITAR components or data contamination limit non-U.S. exports and reduce firm valuation. The presence of components, software, or technical data subject to the ITAR creates significant barriers for Canadian firms seeking to export their products to countries other than the U.S. ITAR restrictions mean that any product incorporating such controlled items is subject to strict licensing requirements and may be denied export approval altogether for certain destinations.

This not only constrains market access but also complicates partnerships with foreign customers and allied governments. Furthermore, ITAR contamination can deter potential investors and buyers, as the compliance burden and legal risks associated with U.S. export controls can negatively impact a firm's attractiveness and valuation. For small and medium-sized enterprises (SMEs), these limitations can severely restrict growth opportunities and undermine competitiveness in the global defence and security markets.

[2] *A patent box is a tax incentive program designed to encourage companies to commercialize their innovations and intellectual property within Canada. Under such a regime, income earned from qualifying patents or other types of intellectual property is taxed at a lower rate than standard corporate income, making it more attractive for businesses to invest in research and development domestically. While some Canadian provinces, such as Quebec, have implemented their own versions of a patent box, a federal-level program is still under consideration to further stimulate innovation and support the growth of Canadian technology companies.*

(continued from previous page)

What needs to change:

- **Canadian ITAR-Avoidance Advisory Cell.** Guidance on "designing out" ITAR, including component substitution and segregation of U.S.-origin technical data.
- **"Controlled but Exportable" Canadian Classification.** A national control tier that retains security oversight while enabling allied exports, aligned with NATO norms.
- **Bilateral Carve-outs.** Pursue targeted arrangements with trusted allies for reciprocal treatment of non-ITAR controlled items.

ACADEMIA-SME COLLABORATION

Inconsistent university IP policies create delays and ownership ambiguity. When universities and SMEs collaborate on research and development projects, differing approaches to intellectual property management can lead to protracted negotiations and confusion over who ultimately owns or controls the resulting innovations. Some institutions may default to university ownership of background and foreground IP, while others negotiate on a case-by-case basis, resulting in a lack of predictability for industry partners.

This patchwork of policies often causes bottlenecks at the contract stage, delays the start of collaborative projects, and can even discourage SMEs from engaging with academic partners due to concerns about future commercialization rights and revenue sharing. As a result, valuable research outcomes may be delayed in reaching the marketplace, hindering the competitiveness of Canadian innovators and slowing the overall pace of technology transfer.

What needs to change:

- **Standardized Defence-Friendly Templates.** Default SME ownership for background IP; foreground on a case-by-case licence basis, royalty-bearing after commercial success thresholds.
- **Defence Research Enclaves.** Secure compute and data enclaves for sensitive projects with vetted access.
- **Embedded Fellowships.** Graduate researchers seconded into SMEs with clear IP pre-assignment.

CYBERSECURITY, GOVERNANCE, AND INSIDER THREATS

As SMEs grow and take on more complex or sensitive projects—particularly in the defence and security sectors—they become increasingly attractive targets for cyberattacks and insider threats. Unlike large corporations, SMEs often do not have the resources or infrastructure to implement robust, enterprise-grade security controls, such as advanced threat detection systems, continuous monitoring, and comprehensive employee vetting procedures. This gap leaves them more vulnerable to data breaches, intellectual property theft – which becomes more important with use of trade secret for software solutions - , and sabotage from both external actors and internal staff.

As their scale increases, so does their exposure: more employees, more partners, and larger digital footprints multiply the potential avenues for attackers. Without adequate support and standardized practices, SMEs may struggle to meet the stringent security requirements of government contracts or collaborative research, ultimately putting valuable innovations and sensitive information at risk and potentially jeopardizing their eligibility for future opportunities.

(continued from previous page)

What needs to change:

- **Cybersecurity Maturity Model Certification (CMMC)-Aligned Baselines.** Subsidized audits and controls tied to contract eligibility.
- **Secure DevSecOps Pipelines.** Federally supported pipelines and code-signing for classified or export-controlled work.
- **Trade-Secret Governance.** Funded audits, access controls, and incident response playbooks.

Implementation Roadmap

A three-phase plan aligns actions, owners, and metrics, while integrating economic/sovereignty benefits and proactive risk management.

PHASE 1: DAY 0-90

Signal, Safeguard, and Set-Up

KPIs (90 days)

- Interim guidance issued
- Number of contracts using purpose-bound licence
- Pilot cohort launched
- Task force charter approved
- Voucher program open.

- ☐ **Interim SME-Safe IP Guidance.** DND and PSPC issue guidance clarifying that background IP remains with SMEs; reach-through requires ADM-level approval. (Owner: DND/PSPC; Support: TBS, CIPO)
- ☐ **Purpose-Bound IP Licences.** Mandate limited, purpose-bound licences on SME contracts below a defined threshold; replace default ownership transfer provisions. (Owner: PSPC; Support: DND legal)
- ☐ **Pilot "Government as First Customer Plus."** Link Innovative Solutions Canada pilots to follow-on DND procurements for Ottawa-headquartered SMEs. (Owner: ISED/DND)
- ☐ **Defence Patent Box Options.** ISED and Finance produce design options modelled on Quebec's regime for fall fiscal update. (Owner: ISED/Finance)
- ☐ **Defence SME IP Task Force.** Interdepartmental task force (DND, PSPC, ISED, TBS, CIPO) to deliver standardized language and training plan. (Owner: DND ADM(Mat)/PSPC Acquisitions)
- ☐ **Targeted Vouchers.** Announce vouchers for cybersecurity (International Organization for Standardization (ISO) 27001, CMMC-aligned) and IP governance (trade-secret frameworks, secure enclaves). (Owner: ISED)

Risk Mitigations:
Template library to reduce legal friction with rapid arbitration protocol for clause disputes.

Economic/Sovereignty Signals:
Template library to reduce legal friction with rapid arbitration protocol for clause disputes.

Build, Standardize, and Start Scaling

KPIs (12-month)

- ≥70% of SME contracts under threshold using purpose-bound licence;
- ≥12 projects bridged from pilot to production;
- neutral arbitration panel established and used at least twice;
- two universities live with defence enclaves;
- Hub operational with ≥50 firms served;
- ≥$X million in export leads facilitated (non-ITAR markets).
- Number of government stakeholders and entrepreneurs changes

- ☐ **Model Contracts & SACC Rewrite.** Publish model SME-safe contracts; implement background-IP exclusion schedules; integrate IP risk checklists into procurement plans. (Owner: PSPC; Support: DND)
- ☐ **Operational Transition Mechanics.** Automatic Phase II/III bridges with named CAF sponsors and minimum fleet-adoption thresholds; create a pathway for justified sole-source conversions from innovation contracts. (Owner: DND)
- ☐ **IP literacy.** Deploy IP training for government stakeholders and entrepreneur covering all types of IP and including the importance of IP clauses in the procurement contracts (and explaining the templates). There should be a common understanding of the new framework and the importance of the IP clauses in the contracts (Owner: ISED)
- ☐ **Fair-IP Conduct & Disclosure.** Require prime disclosure of any reach-through language at bid; integrate SME-protection scoring into evaluation; stand up neutral IP arbitration. (Owner: PSPC; Support: ISED)
- ☐ **Academia Templates & Enclaves.** Adopt standardized defence-friendly IP templates and launch secure Defence Research Enclaves at partner universities. (Owner: ISED; Support: DND)
- ☐ **Defence IP & Commercialization Hub (Ottawa).** Stand-up with co-located IP, export, security, and procurement experts; prepare "deal-ready" IP packages for allies/NATO DIANA. (Owner: ISED; Support: Global Affairs Canada (GAC), DND)

Risk Mitigations:

- Prime resistance → tie ITB multipliers and eligibility to partnering metrics;
- Policy drift → TBS directive on IP carve-outs;
- Talent gaps → training and secondments.

Economic/Sovereignty Signals:

Measurable reduction in foreign dependency for priority C4ISR/AI capabilities with increased SME valuations and investment readiness.

PHASE 3: MONTH 12-24

Institutionalize, Incent, and Internalize

KPIs (24-month)

- ≥35 production contracts transitioned from pilots;
- ≥60% reduction in reported background-IP disputes;
- ≥3 bilateral carve-out MOUs;
- ≥$Y million/year in defence IP licensing revenue reported domestically;
- CAF reports reduced upgrade cycle times for key software-defined systems.

- ☐ **Treasury Board Carve-Outs.** Codify SME IP carve-outs; prohibit background-IP reach-through; create a register of SME-retained defence IP. (Owner: TBS/CIPO)
- ☐ **Patent Box Legislation.** Implement Canadian defence patent box with software/data eligibility and security assurances; pair with accelerated R&D depreciation. (Owner: Finance/ISED)
- ☐ **ITAR-Avoidance & Allied Carve-Outs.** Launch advisory cell, fund ITAR-free design pathways, pursue bilateral carve-outs with trusted allies; align a "Controlled but Exportable" tier with NATO norms. (Owner: GAC/ISED; Support: DND)
- ☐ **Government IP Literacy.** Certify procurement/IP cadres; embed IP CoE (Centre of Excellence) checklists in approvals; rotate officials through SMEs. (Owner: DND/PSPC/ISED)

Risk Mitigations:

- Export pushback → "Controlled but Exportable" guardrails;
- Budget pressure → reallocate within existing programs;
- Legal complexity → staged implementation and sandboxing.

Economic/Sovereignty Signals:

Recurring IP income for SME. Greater CAF agility and resilience against foreign acquisition/ offshoring of critical capabilities.

Summary of Recommendations

GOVERNMENT POLICIES

1. **SME-Safe Defence IP Contracting.** Mandate SME-protective for background and foreground IP clauses under defined thresholds; require Assistant Deputy Minister (ADM)-level justification for deviations; publish model contracts; embed IP specialists within DND project teams.
2. **Government as First Customer Plus.** Guarantee minimum contract values; provide export reference letters; include performance-triggered option years; enable CAF repeat purchases without re-tendering.
3. **Defence SME IP Carve-Outs.** Codify in Treasury Board of Canada Secretariat (TBS) policy; prohibit background-IP reach-through; register SME-retained IP; align with NATO Small Business Innovation Research (SBIR) and European Defence Fund (EDF) models.

4. **Canadian Defence Patent Box.** Reduced rates on qualifying IP licensing and export income, inclusive of software and data-driven IP; require Canadian control and security assurances; pair with accelerated research and development (R&D) depreciation.
5. **IP Literacy.** Mandatory competency certification for government stakeholders and entrepreneurs; Defence IP Centre of Excellence; IP checklists in procurement approvals; rotational placements of officials into SMEs.
6. **Funding IP and Security Governance.** IP protection vouchers; secure DevSecOps; treat IP governance as an eligible security cost; extend supports beyond early stage.

ECOSYSTEM MEASURES

7. **Fair Partnering with SMEs.** Model prime–SME IP agreements; eligibility tied to partnering record; SME satisfaction metrics in ITB evaluations; incent co-investment over acquisition.
8. **Defence IP & Commercialization Hub (Ottawa).** Co-locate IP, export, security, and procurement expertise; provide classified advisory services; package deal-ready IP for allies; act as a NATO Defence Innovation Accelerator for the North Atlantic (DIANA) gateway.

Summary

Retaining intellectual property drives recurring revenue through export and licensing, while also supporting the survival and growth of SMEs, which in turn boosts tax receipts and creates high-value jobs. Enhanced industrial depth, achieved through stronger bargaining positions and equitable partnerships, leads to a more resilient supply chain and less reliance on single prime contractors. Furthermore, Canadian sovereignty and operational readiness are bolstered by maintaining domestic control over IP, which allows for rapid, independent updates and patching during crises and mitigates risks associated with foreign export restrictions.

The proposed measures offer diverse benefits and considerations for stakeholders across the defence innovation ecosystem. For SMEs, they introduce clearer IP rules, expedited pathways to transition technologies, a diminished legal burden, and improved access to capital leveraging their IP assets. Prime contractors benefit from heightened transparency and expectations of fair conduct, receiving incentives—such as ITB multipliers—for safeguarding SME IP and engaging in co-investment. Government departments, including the DND, PSPC, ISED, Treasury Board of Canada Secretariat (TBS), and the Canadian Intellectual Property Office (CIPO), will need to invest in training, adopt model contract clauses, and enhance oversight; in return, they can expect more efficient procurements and reduced disputes. Academia stands to gain from standardized agreement templates and commercialization-linked multipliers, which better align academic incentives with mission-driven outcomes.

There are three principal approaches to advancing the defence innovation ecosystem, each with its own trade-offs. First, taking no action requires minimal effort but would result in ongoing IP leakage, stalled technology transitions, and increased dependence of the CAF on non-sovereign suppliers—a scenario that is not recommended. Second, implementing only a partial contracting fix would improve IP protections but would not deliver significant scaling or export benefits in the absence of complementary measures such as a patent box regime, a dedicated hub, and strategies to avoid ITAR restrictions; this option is considered insufficient. The recommended approach is to pursue an integrated package that combines contracting reform with targeted incentives and the establishment of capability hubs, offering the most robust path to enhanced readiness, sovereignty, and sustainable growth.

The communications and engagement strategy to present the recommended changes should highlight Canada's commitment to safeguarding and expanding domestic defence innovation, ensuring optimal benefits for the Canadian Armed Forces and taxpayers. Key audiences include SMEs, prime contractors, academic institutions, investors, allied countries, and government departments such as DND, PSPC, ISED, TBS, CIPO, and GAC. Early proof points for the initiative encompass issuing interim guidance, launching a pilot bridge pathway, providing vouchers, forming a dedicated task force, and announcing the establishment of a Defence IP and Commercialization Hub.

APPENDIX A — ACRONYMS

AI – Artificial Intelligence
ADM – Assistant Deputy Minister
CAF – Canadian Armed Forces
C4ISR – Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance
CIPO – Canadian Intellectual Property Office
CMMC – Cybersecurity Maturity Model Certification
DND – Department of National Defence
DIANA – Defence Innovation Accelerator for the North Atlantic;
EDF – European Defence Fund
GAC – Global Affairs Canada
IP – Intellectual Property
ISED – Innovation, Science and Economic Development Canada
ISO – International Organization for Standardization
ITAR – International Traffic in Arms Regulations
ITB – Industrial and Technological Benefits
NATO – North Atlantic Treaty Organization
PSPC – Public Services and Procurement Canada
R&D – Research and Development;
SACC – Standard Acquisition Clauses and Conditions
SBIR – Small Business Innovation Research
SME – Small and Medium-Sized Enterprise