CANADIAN GLOBAL AFFAIRS INSTITUTE
INSTITUT CANADIEN DES AFFAIRES MONDIALES

Aligning Canada's Policy Architecture with the Defence Industrial Strategy

By *VAdm (Ret'd)* Ron Lloyd

April 2026

POLICY PERSPECTIVE

Aligning Canada's Policy Architecture with the Defence Industrial Strategy

by

VAdm (Ret'd) Ron Lloyd

April 2026

CANADIAN GLOBAL AFFAIRS INSTITUTE
INSTITUT CANADIEN DES AFFAIRES MONDIALES

Prepared for the Canadian Global Affairs Institute

Suite 2720, 700– 9th Avenue SW., Calgary, AB T9P 3V4

www.cgai.ca

The recently announced Defence Industrial Strategy (DIS) sets out an ambitious vision for expanding Canada's industrial base and strengthening sovereign capability. It arrives at a moment of geopolitical disruption and renewed recognition that sovereign capability depends not only on procurement budgets, but on the policy architecture that enables execution. If those enabling instruments remain unchanged, the DIS risks becoming another well-articulated strategy constrained by the very systems meant to enable it. Strategy can signal intent; only structural alignment delivers capability.

At its core, the DIS is a sovereignty project. For decades, Canada operated within the strategic comfort of proximity to the United States. That environment has shifted. Sovereignty is no longer assumed; it must be sustained through institutional capability. In earlier eras, railways and highways integrated Canada's geography and commerce, binding a vast federation into a functioning economic whole. Today, the decisive infrastructure is institutional rather than physical. Sovereignty depends on whether Canada's governance architecture can move trusted data, allocate risk proportionally and translate strategic ambition into delivered capability at speed.

The challenge is not primarily technological. Canada has capable public servants, sophisticated firms and advanced digital tools. The constraint is structural. When security classification frameworks, accreditation regimes, export controls, contract security requirements and digital governance authorities remain calibrated for a prior era, they become binding constraints on delivery. The objective is not deregulation, but proportional alignment, concentrating safeguards where risk is real while restoring execution speed where it is not. Without that adjustment, additional funding or new strategy cannot produce results reliably.

Over the past several years, the 2025 Digitalizing for Defence Series examined structural impediments across defence, digital governance, industrial participation and central agency policy frameworks. Each addressed a distinct domain. Together, they describe a consistent pattern: Canada's 'small-p' policy architecture, the non-legislated directives, accreditation regimes, oversight instruments that govern daily institutional behaviour, is increasingly misaligned with its strategic ambition. Whether the objective is defence industrial expansion, critical minerals development, sovereign Artificial Intelligence (AI), or major project acceleration, execution ultimately runs through the same federal policy architecture.

These instruments shape the speed and cost of execution. When clearance timelines lengthen, digital adoption stalls, or compliance requirements become disproportionate, the effect is cumulative. Institutional friction translates into delayed procurement, slower service modernization, reduced small- and medium-sized enterprise (SME) participation and diminished economic velocity. Canada's decline in the United Nations E-Government Development Index, from 3rd in 2010 to 47th in 2024, reflects not a shortage of talent or ambition but an institutional coherence problem.

Recent discussions at the Canadian Digital Council Executive Forum on Digital Sovereignty underscore the importance of provincial dynamics. In a federation, digital sovereignty cannot be federally imposed; it must be interoperable. However, federation alignment is dependent upon prior federal coherence. Without proportional calibration of federal classification, cyber and assurance frameworks, intergovernmental interoperability risks exporting existing structural friction across jurisdictions rather than resolving it.

Federated countries such as Australia and Germany have approached digital integration deliberately, but in each case federal governance instruments were first recalibrated to enable proportional risk alignment. Interoperability without federal coherence does not accelerate delivery; it compounds complexity.

Canada's path to digital sovereignty therefore begins with structural reform at the federal level. Once foundational policy instruments are proportionally aligned, federation-wide interoperability becomes not only feasible but economically transformative. A First Ministers' commitment to reduce internal digital barriers as decisively as internal trade barriers would strengthen labour mobility, reduce compliance duplication and unlock productivity gains across jurisdictions.

Lower friction increases economic velocity. Trusted digital identity reduces fraud and reinforces the sovereignty of citizen-state interactions. Shared authentication and assurance standards enable secure data exchange, improve service delivery and reduce redundant oversight regimes. Interoperability strengthens resilience by ensuring that disruption in one jurisdiction does not fragment the whole. Properly designed, federation alignment is not a technical exercise; it is a national competitiveness strategy. In the twenty-first century, national unity is reinforced not only by highways and pipelines, but by interoperable digital systems.

The same structural pattern is visible in defence industrial policy. Canadian founders seeking to provide advanced capabilities to the Canadian Armed Forces (CAF) demonstrate technological sophistication. Their principal barriers were not innovation gaps but policy friction, prolonged security clearance processes, rigid contract security requirements, cyber certification burdens, and export control constraints.

The recently announced DIS articulates sound objectives: expand the industrial base; accelerate SME participation; enable iterative capability development; and strengthen exports. There is little disagreement with these aims. The constraint is execution.

Many of the policy levers that determine whether those objectives can be realized reside within functional authorities such as the Treasury Board Secretariat (TBS), Communications Security Establishment (CSE), Shared Services Canada (SSC) and the Royal Canadian Mounted Police (RCMP) rather than the delivery departments. These functional authorities operate largely outside the formal scope of the DIS, yet they determine whether its objectives are achievable

within acceptable timelines and cost. Without their alignment, delivery departments cannot overcome structural delay.

When the policy instruments managed by these institutions remain misaligned and risk-averse, delivery departments remain constrained regardless of funding levels or strategic intent. The consequence is measurable delay. Additional months in clearance processes, incremental compliance costs for firms, and extended approval cycles for digital adoption compound over time. The result is slower procurement, reduced industrial participation and diminished agility. Over time, structural delays do more than slow execution; it erodes strategic ambition itself. When year after year of friction prevents delivery at pace, governments are eventually forced to reset strategy rather than realize it. In that sense, speed is not cosmetic; it is strategic.

These are not dramatic reforms. They are structural ones. They determine whether strategy translates into capability.

The familiar adage that culture eats strategy for breakfast has become a convenient explanation for implementation failure. In practice, small-p policy defines culture. Classification frameworks, cyber controls, contract security instruments, export regimes and oversight authorities establish the incentives and constraints that govern daily institutional behaviour. When those embedded rules remain unchanged, they will quietly neutralize any strategy misaligned with them. Strategy does not fail because culture resists it. Strategy fails when the policy architecture that shapes culture remains untouched.

Structural reform strengthens, rather than weakens, Canada's national security posture. Overclassification and disproportionate assurance regimes do not increase security; they diffuse attention and slow delivery. When low-risk activity is subjected to controls designed for high-risk environments, two systemic effects occur: execution slows; and oversight focus disperses. Proportional alignment concentrates safeguards where they matter most and restores execution speed as a component of sovereignty.

From Strategic Intent to Measurable Delivery

The Digitalizing for Defence Series underlying this article is intentionally detailed. It is written to equip leaders with the substance required to challenge advice that defaults to the status quo. The analysis presented here is not offered as a matter of opinion. It is testable. If implementation does not improve procurement velocity, SME participation and digital adoption timelines within measurable periods, the diagnosis will have been incorrect. If it does, the constraint will have been structural rather than strategic.

For that reason, this work does not stop at diagnosis. The recommendations emerging from the Digitalizing for Defence Series are consolidated in a unified annex and accompanied by a sequenced implementation roadmap. Together, they translate analysis into a practical framework for delivery, with clear decision points, ownership and time horizons.

These tools are intended to be useful not only to those charged with implementation inside government, but also to parliamentarians, committees, journalists and academics whose roles include scrutiny, oversight and informed public debate. By making assumptions, dependencies and sequencing explicit, the annex and roadmap provide a common reference point against which progress, or the lack of it, can be assessed over time. In that sense, the framework is deliberately transparent, designed to support accountability and learning rather than to advance any particular institutional or partisan position.

Analytical Framing of the Digitalizing for Defence Series

The papers that underpin this blueprint examine multiple domains, defence, digital governance, industrial policy and central agency frameworks. While each address a distinct policy area, they share a common analytical foundation.

First, they posit that policy architecture can act as a binding constraint on delivery. Funding, workforce capacity and leadership all influence outcomes. However, when risk frameworks, accreditation regimes and governance instruments are misaligned with strategic ambition, additional investment cannot reliably translate into measurable results. The emphasis throughout the prior work has therefore been structural rather than programmatic.

Second, defence was used deliberately as a stress test rather than treated as an exceptional case. Defence sits at the intersection of high assurance requirements, digital integration, industrial participation and allied interoperability. Institutional frictions that surface in defence typically reveal broader systemic dynamics. The patterns identified were intended to illuminate cross-government architecture, not isolate a single portfolio.

Third, allied comparisons help demonstrate feasibility and proportionality, not advocate replication. Differences in constitutional structure and administrative culture are acknowledged. The consistent observation across allied practice is not uniformity of model, but clarity of responsibility, risk-tiering and continuous improvement and calibration of safeguards as technology evolves.

Fourth, risk is allocative rather than eliminable. Governance systems that prioritize minimizing institutional exposure can inadvertently increase operational risk borne by delivery organizations. The central question has been whether risk is currently positioned where it best serves Canada's strategic interests.

Finally, the analysis has not assumed frictionless reform. Horizontal change across security, digital, procurement and industrial policy is complex. The intent has been to make structural trade-offs visible so that leadership decisions can be taken consciously rather than implicitly through inertia.

The recommendations consolidated in this blueprint are the cumulative expression of that analytical approach.

Annex A. Implementation Logic and Sequencing

The consolidated table identifies the minimum structural adjustments required to realign Canada's governance architecture with strategic ambition. The implementation roadmap that follows provides a sequenced approach to delivery.

Phasing is designed to: (1) reset foundational risk frameworks before downstream instruments are modified; (2) prevent contradictory guidance during transition; (3) assign clear ownership at each stage; and (4) make progress observable within defined time horizons. Execution discipline, not additional strategy articulation, will determine whether Canada's sovereignty objectives are realized in practice. Governments are judged not by the sophistication of their strategies, but by the reliability of their delivery systems. Canada's sovereignty objectives will ultimately be decided by whether its delivery architecture is prepared to evolve.

Table A-1. Consolidated Recommendations Organized by Reform Pillars

Ref	Actionable Decision	Policy / System Lever	Lead Responsibility	Sequencing	Intended Effect
Pillar I. Reset the Security Foundation					
1-A	Adopt modern security classification framework (Official / Official-Sensitive / Secret / Top Secret)	Directive on Security Management Appendix J – Standard on Security Classification	Treasury Board Secretariat (OCIO)	Foundational	Enables alignment with NATO/Five Eyes; resets overclassification culture; unlocks digital and SME reform
1-B	Articulate injury and business-impact models; include examples of business impacts	Risk framework guidance aligned to 1-A	Treasury Board Secretariat (OCIO)	After 1-A	Ends false equivalency; improves classification accuracy
1-C	Retire the Harmonized Threat and Risk Assessment Methodology (TRA-1)	TRA-1	TBS / CSE / RCMP	Foundational	Reduces institutional risk aversion; overlaps with other government risk policy frameworks
1-D	Define aggregation of data in line with allied practice	Clarification alongside 1-A updates	Treasury Board	After 1-A	Enables analytics and AI; clarifies

			Secretariat (OCIO)		risk when datasets are combined
1-E	Explicitly accept transition risk to reduce aggregate risk	Risk culture and governance	Ministers / Deputy Ministers	Continuous	Breaks institutional inertia; enables proportional reform
Pillar II. Modernize Cyber and Digital Architecture					
2-A	Replace ITSG-33 with a consolidated modern IT control framework in keeping with allied best practices	ITSG-33	CSE / TBS	After 1-A	Enables modern digital architectures; removes policy seams
2-B	Explicitly articulate that approved commercial software is acceptable when processing Official/Official-Sensitive data	Codify in ITSG-33 replacement and in 1-A update	TBS / CSE / SSC	Concurrent with 1-A	Reduces cost and improves service delivery without degrading security of citizen data
2-C	Reform CPCSC] to a risk-based, allied-aligned model that accepts CMMC equivalency	CPCSC	TBS / PSPC / CSE	Foundational (parallel with Pillar I)	Prevents SME exclusion; makes Canadian primes more competitive; maintains security outcomes
2-D	If CPCSC 'alignment' to CMMC remains, limit Level 3 to ~1% of suppliers	CPCSC	DND / PSPC	Linked to 2-C	Ensures only the most sensitive unclassified projects require Level 3; limits disproportionate cost burden
2-E	Adopt Zero Trust and data-centric security explicitly	Codify in ITSG-33 replacement and higher-level cyber policy	CSE / TBS / Public Safety	Linked to 2-A	Modernizes cyber posture and enables secure interoperability
Pillar III. Reform Contract Security					

and Personnel Assurance					
3-A	Align Designated Organization Screening (DOS) with allied practice	Contract Security Program (CSP)	TBS / PSPC	After 1-A	Removes SME barriers while maintaining proportional assurance
3-B	Retain Facility Security Clearance (FSC) rigor for classified procurements	Contract security instruments	PSPC	After 1-A	Focuses high assurance where risk is real
3-C	Replace clearance reliance with information-handling training for low-risk work	Personnel assurance and training standards	PSPC / TBS	After 1-A	Improves behavioural risk mitigation; reduces unnecessary clearance delays
3-D	Reallocate CSP resources toward FOCI and high-risk activity	Program design and resourcing	PSPC	After 1-A	Improves security outcomes by focusing on the highest-risk vectors
3-E	Reduce reliability screening look-back periods (UK-aligned)	Personnel security policy	TBS	Independent	Improves talent access and hiring velocity
3-F	Make departments accountable for contractor screening issuance where required	Governance and accountability	Departments / TBS	Independent	Aligns risk ownership with delivery responsibility
Pillar IV. Restore Defence Institutional Authority					
4-A	Permit Defence to host and manage all of its data and acquire software applications based on its requirements	Digital authority	TBS / DND	After 1-A to 2-B	Enables risk owners (CDS/DM) to best manage and mitigate risk; does away with the false dichotomy of administration vs

					operational data; restores agility; reduces dependency-induced friction
4-B	Amend OIC 2015-1071to remove Defence's dependency on SSC	OIC 2015-1071	PCO / TBS	After 2-A	Enables Defence to leverage SSC where it best makes sense for Defence
Pillar V. Align Trade and Industrial Security with Allies					
5-A	Publish and track industry compliance costs	Transparency and reporting	PSPC / TBS	Independent	Supports evidence-based reform; makes burdens visible
5-B	Integrate export controls and Controlled Goods Program (CGP)	Trade control modernization	GAC / DND	After 1-A	Removes SME bottlenecks; improves competitiveness
5-C	Modernize the Controlled Goods Regulations to enable risk-tiering and digital clarity; assess need for Defence Production Act amendment following implementation	Regulatory amendment (GIC); Legislation if required	PSPC/TBS; Cabinet (if statutory amendment required)	After foundational alignment; concurrent with 5-B integration work	Introduces risk-tiered controls; clarifies digital possession and safeguarding; enables delegated schedule update mechanisms; and preserves full statutory oversight; legislative amendment only if necessary to remove residual authority gaps
5-D	Establish US and Five Eyes assurance gating for streamlined trust	Allied trust mechanisms	PCO / GAC	Continuous	Preserves interoperability and accelerates collaboration
Pillar VI. A National Project:	These measures are contingent upon completion of foundational federal reforms under Pillars I-III. Federation-wide interoperability must build				

Aligning the Federation for Digital Sovereignty (Dependent on Federal Reset)	upon proportionally aligned federal classification, cyber and assurance frameworks to avoid replicating structural friction at greater scale.				
6-A	Launch a First Ministers' Digital Sovereignty Accord	First Ministers' agreement	Prime Minister and Premiers	Initiate concurrent with Pillar I	Establish national commitment to interoperability and proportional risk alignment; elevate digital coherence to parity with internal trade reform
6-B	Create a National Interoperability and Trust Framework (identity, credentialing, secure data exchange)	Shared digital standards	TBS (OCIO) with provincial central agencies	After 1-A and 1-D	Enable cross-jurisdictional service delivery; support labour mobility and productivity; reduce duplicative assurance regimes
6-C	Harmonize risk-tiering and assurance standards across jurisdictions	Common risk calibration guidance	Federal and provincial central agencies	After 1-A	Prevent overclassification spillover; enable shared analytics and AI; improve resilience through common safeguards

Annex B. Implementation Roadmap

Sequenced delivery of actionable decisions to align Canada's defence, digital and industrial foundations.

Phase	Timeframe	Primary Objective	Actionable Decisions	Key Deliverables	Senior Owner(s)
Phase 1	0-90 days	Reset foundational policy drivers of risk aversion and launch federation alignment	1-A, 1-B, 1-C, 1-E	Interim security classification direction; TRA-1 suspension; establish decision log and governance	TBS; PCO
Phase 2	90-180 days	Modernize digital and cyber policy framework and enable proportional adoption	1-D, 2-A, 2-B, 2-E, 3-A, 3-B, 3-C, 3-E, 4-B	Interim ITSG-33 replacement; consolidated cyber guidance; data aggregation clarification; Zero Trust directive; draft interoperability and trust framework	CSE; TBS; PCO
Phase 3	180-365 days	Remove procurement and industry participation barriers; align assurance regimes	2-C, 2-D, 3-D, 3-F, 5-A	Revised CSP guidance; CPCSC scope and phasing decision; published compliance cost baseline; updated supplier onboarding; agreed cross-jurisdiction risk-tier guidance	PSPC; TBS; DND; Provincial central agencies
Phase 4	12-24 months	Restore defence digital autonomy and align trade controls; institutionalize federation governance	4-A, 5-B, 5-C, 5-D, 6-A, 6-B, 6-C	Defence-managed data and cloud operating model; integrated CGP/ECP model; legislative package as required; Five Eyes assurance statements; standing FP digital architecture council operating	PCO; GAC; DND; TBS

List of Acronyms

Acronym	Definition
AI	Artificial Intelligence
CAF	Canadian Armed Forces
CDS	Chief of the Defence Staff
CGP	Controlled Goods Program
CMMC	Cybersecurity Maturity Model Certification (United States Department of Defense program)
CPCSC	Canadian Program for Cyber Security Certification
CSE	Communications Security Establishment
CSP	Contract Security Program
DIS	Defence Industrial Strategy
DM	Deputy Minister
DND	Department of National Defence
DOS	Designated Organization Screening
ECP	Export Controls Program
FOCI	Foreign Ownership, Control or Influence
FSC	Facility Security Clearance
FP	Federal–Provincial
GAC	Global Affairs Canada
GIC	Governor in Council
ITSG-33	Information Technology Security Guidance–33
NATO	North Atlantic Treaty Organization
OCIO	Office of the Chief Information Officer (Government of Canada)
OIC	Order in Council
PCO	Privy Council Office
PSPC	Public Services and Procurement Canada
RCMP	Royal Canadian Mounted Police
SME	Small and Medium-sized Enterprise
SSC	Shared Services Canada
TBS	Treasury Board of Canada Secretariat
TRA-1	Harmonized Threat and Risk Assessment Methodology

About the Author

A native of Taber, Alberta, VAdm (Ret'd) Ron Lloyd was the 35th Commander of the Royal Canadian Navy from 2016-2019. During that time he was also "double hatted" as the acting Vice Chief of the Defence Staff for almost half a year and as the first Chief Data Officer for the Department of National Defence and Canadian Armed Forces for a full year.

During his 38 year career in the RCN, he was privileged to have commanded HMCS CHARLOTTETOWN, HMCS ALGONQUIN, the PACIFIC Fleet and the ATLANTIC fleet. He has extensive operational experience having deployed on numerous occasions globally.

Lloyd has over a decade of experience at National Defence Headquarters having also served as the Deputy Commander of the RCN, the Chief of Force Development for the Canadian Armed Forces, the Director General of Force Development for the RCN and Executive Assistant to the Commander of the RCN.

Lloyd holds a Bachelor of Arts in Military and Strategic Studies from Royal Roads Military College (1985) and a Master of Arts in War Studies from the Royal Military College (2004). He is a graduate of both the Command and Staff Course and the National Security Studies Course at the Canadian Forces College in Toronto. He has also attended the HARVARD Kennedy School, Executive Education, Senior Executives in National and International Security.

Today, as Principal of Leadmark Ventures, he shares his experience in leadership, strategic planning and digital transformation with organizations committed to providing innovative solutions that enhance public sector performance in defence and non- defence related activities.

Canadian Global Affairs Institute

The Canadian Global Affairs Institute focuses on the entire range of Canada's international relations in all its forms including (in partnership with the University of Calgary's School of Public Policy), trade investment and international capacity building. Successor to the Canadian Defence and Foreign Affairs Institute (CDFAI, which was established in 2001), the Institute works to inform Canadians about the importance of having a respected and influential voice in those parts of the globe where Canada has significant interests due to trade and investment, origins of Canada's population, geographic security (and especially security of North America in conjunction with the United States), social development, or the peace and freedom of allied nations. The Institute aims to demonstrate to Canadians the importance of comprehensive foreign, defence and trade policies which both express our values and represent our interests.

The Institute was created to bridge the gap between what Canadians need to know about Canadian international activities and what they do know. Historically Canadians have tended to look abroad out of a search for markets because Canada depends heavily on foreign trade. In the modern post Cold War world, however, global security and stability have become the bedrocks of global commerce and the free movement of people, goods and ideas across international boundaries. Canada has striven to open the world since the 1930s and was a driving factor behind the adoption of the main structures which underpin globalization such as the International Monetary Fund, the World Bank, the World Trade Organization and emerging free trade networks connecting dozens of international economies. The Canadian Global Affairs Institute recognizes Canada's contribution to a globalized world and aims to inform Canadians about Canada's role in that process and the connection between globalization and security.

In all its activities the Institute is a charitable, non-partisan, non-advocacy organization that provides a platform for a variety of viewpoints. It is supported financially by the contributions of individuals, foundations, and corporations. Conclusions or opinions expressed in Institute publications and programs are those of the author(s) and do not necessarily reflect the views of Institute staff, fellows, directors, advisors or any individuals or organizations that provide financial support to, or collaborate with, the Institute.