Forum of Federations
The Global Network on Federalism and Devolved Governance

November 2026

POLICY BRIEF SERIES

GOVERNING ARTIFICIAL INTELLIGENCE IN FEDERAL SYSTEMS

Shared Artificial Intelligence Stewardship and Governance in Canada

Lucie Vignola
Yannick Newton





Shared Artificial Intelligence Stewardship and Governance in Canada

Published By:
Forum of Federations

75 Albert Street, Suite 411
Ottawa, ON K1P 5E7
Canada

www.forumfed.org

Suggested citation:

Vignola, L., & Newton, Y. (2026). *Shared Artificial Intelligence Stewardship and Governance in Canada*. (Governing Artificial Intelligence in Federal Systems) [Forum of Federations Policy Brief] Forum of Federations.

© Forum of Federations, 2026

KEY TAKEAWAY

Canada's AI challenge is a digital federalism challenge: responsible adoption depends on shared infrastructure, common safeguards, coordinated investment, and public-sector capacity across jurisdictions. The central policy lesson is to build interoperable foundations that allow governments to act together where needed while preserving jurisdictional flexibility.

> ***"National AI goals in Canada are only achievable if governments coordinate decisions that are often made separately. The path forward is shared stewardship: common foundations where needed, jurisdictional flexibility where appropriate, and sustained investment in the capabilities that allow governments to act together."***

THE ISSUE

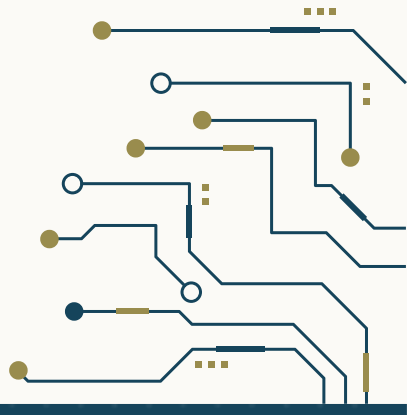
Canada's AI Governance Challenge

Across Canada, governments see AI as an opportunity and a risk. It can improve productivity, reduce costs, enhance efficiency, spur economic growth, and strengthen service delivery yet raises important questions about environmental stewardship, bias, privacy, transparency, and trust. Artificial intelligence is becoming a core part of public services, economic development, scientific research, cyber security, and government operations. **Canada's challenge is not simply regulating AI. It is also governing and using AI across a federation where authority, infrastructure, data, and service responsibilities are shared**. The federal government can set national priorities and fund key capacity, but many other actors shape how AI is adopted. These include provinces, territories, municipalities, Indigenous governments, public agencies, arm's-length institutions, academia, and the private sector. Their decisions affect areas such as health care, education, energy systems, digital infrastructure, procurement, workforce development, and front-line service delivery.

This makes AI governance a federalism issue. AI systems depend on shared foundations like privacy protection, cyber security, common standards, trusted identity, secure data exchange, oversight, and public-sector skills. When these foundations are fragmented, governments must integrate systems. Systems currently continue to be developed for individual program areas, often in individual departments rather than grouped by function. That increases cost, slows adoption, weakens accountability, and makes it harder for people and businesses to receive seamless services across jurisdictions, all of which negatively affect productivity and trust.

Canada has made major commitments to AI. The federal National Artificial Intelligence Strategy: AI for All presents AI as a tool for prosperity, trusted adoption, public benefit, and sovereignty. The Canadian Sovereign AI Compute Strategy commits significant funding to domestic compute infrastructure, public supercomputing capacity, and access to compute for Canadian firms and researchers. These investments recognize that **responsible AI adoption requires more than rules**. **It requires infrastructure, capability, trust, and coordination**.

The policy problem is therefore practical and urgent: how can Canada support AI adoption while preserving public trust, protecting rights, strengthening sovereignty, and respecting the division of powers? The answer is not a single national system or one-size-fits-all model. Canada needs a federated approach that aligns governments around **shared outcomes, minimum safeguards, interoperable systems, and reusable capabilities while leaving room for local needs and jurisdictional choice**.



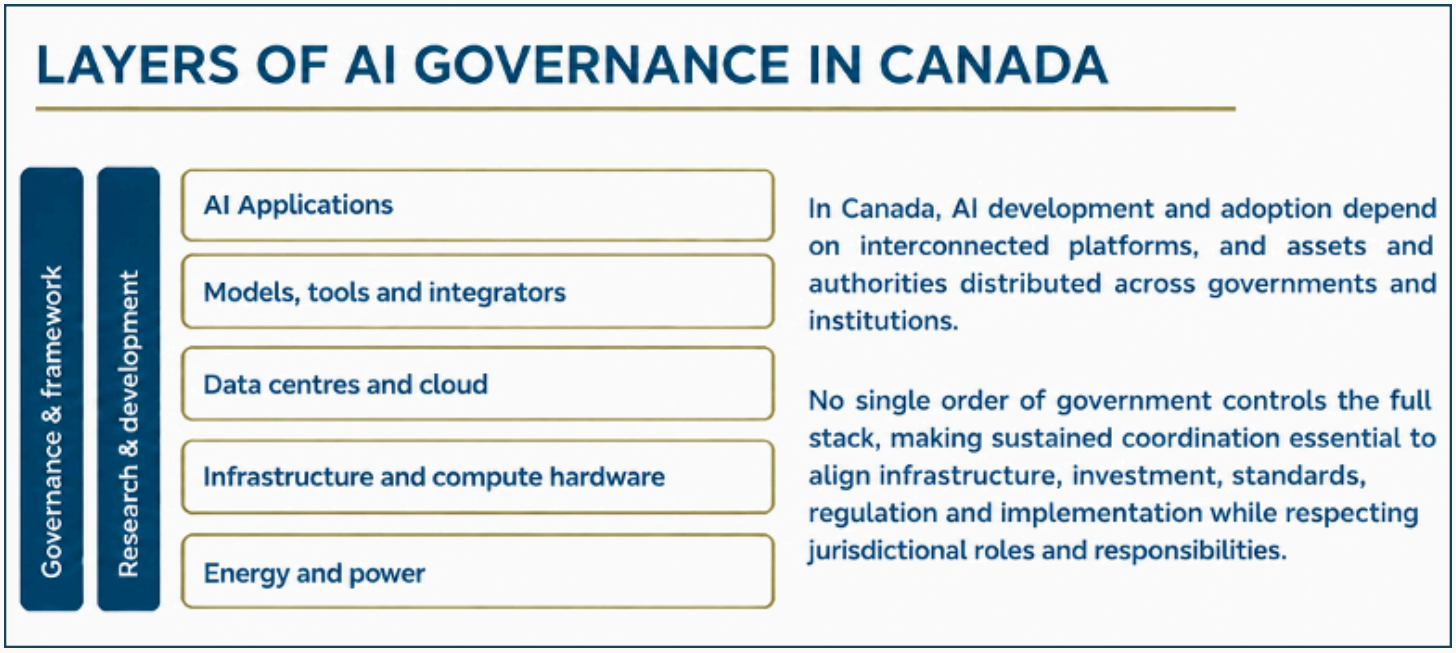
THE FINDINGS

AI Governance in Canada is a Coordination Challenge

Canada's experience shows that AI governance depends less on central control than on sustained coordination among governments and public institutions. Rather than a single centralized system, AI capacity is being developed through a distributed network of institutions, research centres, and partners. At the same time, key enablers: energy systems, nfrastructure and permitting, are largely within provincial and territorial jurisdiction. No single order of government controls all the assets needed for AI adoption. Compute infrastructure, electricity systems, data resources, cyber security, research institutions, procurement rules, skills programs, and public services are spread across the federation.

This means **national AI goals are only achievable if governments align on desired outcomes and coordinate decisions often made separately**.

Ongoing federal - provincial - territorial discussions over the past few years on digital trust, cyber security, digital public infrastructure, sovereign compute, and AI adoption point in the right direction. National ambitions depend on aligning efforts across jurisdictions while respecting roles and responsibilities. Federalism changes what good governance looks like. In a federation, **success depends on aligned policies and legislation, common standards, shared assurance practices, compatible infrastructure, and regular forums** to identify risks, learn from each other, and align investments.



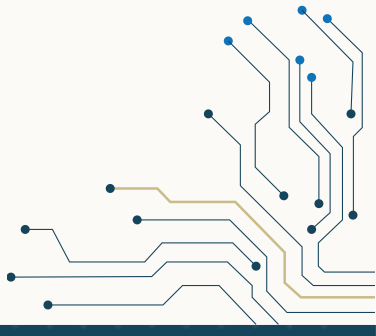
THE FINDINGS

AI Adoption Depends on Shared Digital Foundations

Many AI challenges are digital government challenges. AI systems need reliable data, trusted identity, secure exchange, strong privacy controls, and clear accountability. These are the same foundations needed for integrated digital services. Without them, governments may be able to pilot AI tools, but they will struggle to scale them effectively, efficiently, and securely across programs and jurisdictions.

In a federation, **interoperability matters more than uniformity**. Canada does not need every government to use the same technology or service model. It does need systems that can work together when people, data, risks, and responsibilities cross boundaries. This requires aligned legislation, common technical and policy standards, clear decision rights, and shared governance for high-value capabilities such as digital identity, consent, data exchange, assurance, and reusable platforms. Beyond these systems, a shift in public administration is needed. Traditional Westminster systems are built around vertical accountability, departmental authority, and careful control of information. Those values remain important, but AI and digital services need horizontal design to lead to meaningful positive outcomes. **Governments need mechanisms that enable responsible information sharing, joint risk management, and coordinated delivery while preserving accountability** to ministers, legislatures, and the public.

Canada has strong, autonomous levels of government. As many public policy issues involve different levels of government, intergovernmental relations have been key in addressing issues, managing crises, and collaborating on cross-jurisdictional priorities. Each government has intergovernmental teams to help align on, and support, broader initiatives. There are federal, provincial, and territorial ministerial and deputy ministerial fora that are held regularly. These fora are supported internally (usually by a chair's department or agency) or by organisations like the Institute for Citizen-Centred Service for strategic planning and enablement. They also benefit from logistical support by the Canadian Intergovernmental Conference Secretariat. The main ecosystem exists. And yet, AI cuts across every sector of government and touches an endless number of files, (e.g. sovereignty, digital transformation, economic resilience, public trust, public-sector capability). A more robust and integrated approach is needed to address the wide-ranging socio-economic impacts of AI. Closer alignment would increase opportunities to make meaningful progress on shared goals and outcomes for the country. It would also help avoid duplication of efforts and resources as well as incomplete and fragmented briefings that increase the risk of unintended consequences of AI use and implementation.



THE FINDINGS

AI Sovereignty Means Building Shared, Self-Reliant Capacity

Canada's AI strategy and compute investments show that sovereignty is central to AI policy. In this context, sovereignty does not mean doing everything in Canada or avoiding global partners. It means building enough Canadian capability, industry, knowledge, infrastructure access, procurement strength, and governance capacity to make important choices on public terms. The goal is self-reliance where it matters most, not full independence from the global technology market.

As in other areas, the conditions for sovereign AI capacity are shared across governments. Federal funding can support national compute infrastructure and research capacity, including through the AI Sovereign Compute Infrastructure Program and the federal initiative to build large-scale AI supercomputing capacity. Provinces and territories shape electricity supply, data-centre approvals, local infrastructure, skills, innovation ecosystems, and many public-sector use cases. Alberta's focus on AI data centres, Ontario's emphasis on compute, clean energy, and critical technologies, and British Columbia's use of clean-power allocation for high-load industries show that provincial decisions affect Canada's ability to build AI capacity in a sovereign and practical way.

The lesson for Canada is clear: **AI sovereignty should be treated as shared stewardship**. It includes compute, cloud, cyber security, digital identity, data governance, procurement, intellectual property, public-sector skills, and vendor dependence. Strong national capacity requires aligned investments across governments so Canada can remain self-reliant in critical areas while still working with trusted partners.

Governments Need More Transparent Measures of AI and Digital Maturity

Current digital government rankings often treat countries as unified systems. That approach misses a central challenge in federations: whether people can move across services and jurisdictions without repeated data entry, inconsistent identity requirements, fragmented service channels, or unresolved handoffs. For AI, governments should measure not only adoption, pilots, efficiencies, or spending, but also whether systems improve real service outcomes across boundaries. They should also measure whether the public is aware and understands how AI is being used, tested, monitored, governed, and verified.

Useful measures would include whether: identity and consent systems work across jurisdictions; data can be exchanged securely and appropriately; AI tools are tested, monitored, documented, and reviewed by humans before important decisions are made; public servants have guidance and training; transparency requirements are clear, and shared capabilities are funded for the long term. In federal systems, the most important measure is not whether one government is digitally advanced, but if the federation can deliver trusted services when responsibilities are shared, explain those services clearly to the public, and show where human judgment remains accountable for decisions.

THE FINDINGS

Trust, Privacy, Security, and Workforce Guidance are Conditions for Adoption

Public trust is not a communications issue after AI systems are deployed; it is a condition for adoption from the start. People need confidence that AI-supported services are free of bias, lawful, fair, explainable, secure, and subject to human oversight. The Office of the Privacy Commissioner of Canada's guidance on privacy and generative AI emphasizes accountability, transparency, necessity, proportionality, and lawful handling of personal information. These principles should be treated as operating requirements, not optional safeguards.

AI also changes cyber risk. Canadian cyber security guidance, including the Canadian Centre for Cyber Security's Guidelines for Secure AI System Development and Top 10 Artificial Intelligence Security Actions, highlights risks such as prompt injection, data poisoning, unauthorized disclosure, model compromise, adversarial use of AI, and overreliance on generated outputs. These risks do not stop at jurisdictional borders. A weak practice in one organization can affect public confidence in governments and AI-enabled services more broadly. This creates **a strong case for shared assurance, common risk language, coordinated incident response, and regular testing across governments**.

Responsible adoption also depends on public servants. Many AI risks emerge through everyday use: entering sensitive information into tools, relying on outputs without review, using models outside approved settings, or failing to identify bias and error. Treasury Board of Canada Secretariat guidance on generative AI, automated decision-making, and the AI Strategy for the Federal Public Service 2025–2027 provides a useful operational model. Other jurisdictions can adapt this approach by combining clear rules, practical examples, training, communities of practice, and escalation pathways for high-risk use cases.

> ***"Risks do not stop at jurisdictional borders. A weak practice in one organization can affect public confidence in governments and AI-enabled services more broadly. Strong national capacity requires aligned investments across governments so Canada can remain self-reliant in critical areas while still working with trusted partners."***

POLICY LESSONS

Putting it all Together

What does this mean on a federalism level? **Closer collaboration, new ways of working together, and less diffusion in effort and resources are needed**. The adoption and deployment of AI exemplify how one sector or issue can increasingly cut across multiple jurisdictions and multiple federal, provincial, and territorial fora. AI is intertwined with several sectors, including digital infrastructure, cyber security, economic development, sovereignty, procurement, environment, digital government, privacy, discrimination, and public trust. A new way of approaching intergovernmental affairs is needed—within individual jurisdictions as well as between jurisdictions— so existing fora can operate more strategically and coherently with better use of resources. To achieve this, special attention should be paid to the following policy issues:

- **Treat AI governance as shared federated stewardship, not a single-government responsibility**

Canada's AI capacity depends on decisions made across federal, provincial, territorial, municipal, Indigenous, public-sector, academic, and private-sector systems. Governments should use standing federal/provincial/territorial mechanisms to align priorities, share risks, coordinate investment, and support consistent safeguards while preserving jurisdictional flexibility.

- **Build common digital foundations before scaling AI**

AI adoption will not scale safely without trusted identity, secure data exchange, privacy protection, cyber security, consent management, documentation, and human oversight. These foundations should be designed as reusable public infrastructure rather than rebuilt program by program.

- **Focus on interoperability, not uniformity**

Canada does not need every jurisdiction to use the same tools, platforms, or service models. It does need systems that can work together when people, data, risks, and responsibilities cross borders. Governments should agree on minimum standards and shared assurance practices while allowing local implementation choices.

- **Make AI sovereignty a practical capacity agenda**

Sovereignty should mean having enough Canadian compute, cloud access, procurement leverage, cyber security capability, data governance, public-sector expertise, and vendor management capacity to make key decisions on public terms. Federal investments should be aligned with provincial and territorial roles in energy, infrastructure, skills, and service delivery.

POLICY LESSONS

- **Treat trust, privacy, and cyber security as adoption requirements**

Privacy assessment, security testing, transparency, bias review, monitoring, and clear accountability should be built into AI projects as they are being developed, long before they scale. These safeguards should not be treated as compliance steps after deployment but rather as keys to success. Working through the different levels of government can ensure affected internal and external stakeholders are involved and considered from the beginning.

- **Invest in public-sector workforce guidance and responsible use**

Public servants need practical, role-based guidance on when and how AI can be used, how to protect sensitive information, how to verify outputs, when to escalate risks, and how to manage procurement or vendor tools. Training should be tied to real service contexts, not generic awareness alone. Rather than developing individual approaches, collaboration would lead to consistency and interoperability beyond simply the technical level.

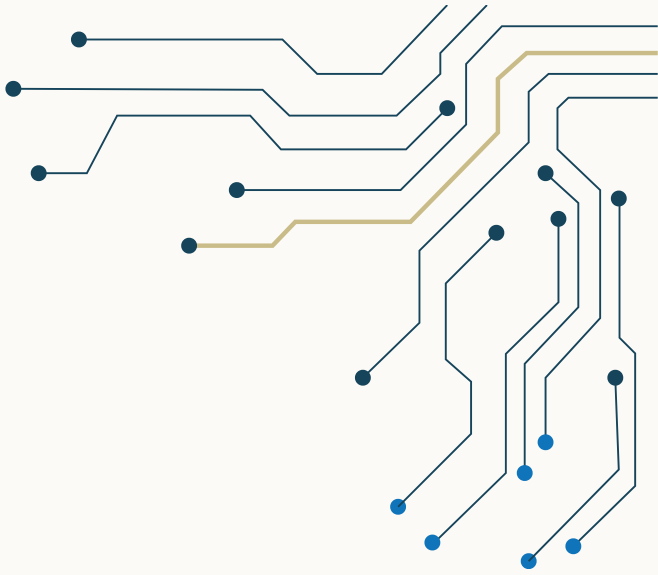
- **Measure AI success through pan-Canadian public outcomes**

Governments should track whether AI improves service quality, reduces duplication, strengthens cross-jurisdictional delivery, protects rights, improves public trust, and preserves public control over critical capabilities. In a federation, the key test is whether people experience simpler, safer, and more coherent services across government boundaries.

- **Be transparent with the public about how AI is used**

Governments should clearly explain when AI supports public services, what data is used, what safeguards are in place, how decisions are reviewed, and where human accountability remains. Public understanding is essential to trust and adoption.

The central lesson is clear: Canada's AI challenge is also **a digital federalism challenge**. AI will only be as trusted, secure, interoperable, and useful as the public infrastructure and governance arrangements beneath it. **For Canada and other federal systems, the path forward is shared stewardship: common foundations where needed, jurisdictional flexibility where appropriate, and sustained investment in the capabilities that allow governments to act together**.



References

Canadian Centre for Cyber Security. (2023). *Guidelines for Secure AI System Development*.

Canadian Centre for Cyber Security. (2026). *Top 10 Artificial Intelligence Security Actions: A Primer*.

Government of Alberta. (2024). *Artificial Intelligence Data Centres Strategy*.

Government of Alberta. (2025). *Powering New Pathways for Data Centres*.

Government of British Columbia. (2026). *B.C. Launching Competitive Process for Clean Power in High Load Industries*.

Government of Canada. (2021). *Distribution of Legislative Powers in Canada*.

Government of Newfoundland and Labrador. *Digital Trust and Cyber Security Priorities Discussed at Annual Meeting of Federal, Provincial and Territorial Ministers*.

Canadian Intergovernmental Conference Secretariat. *Digital Trust and Cyber Security Priorities Discussed at Annual Meeting of Federal-Provincial-Territorial Ministers*.

Canadian Intergovernmental Conference Secretariat. *Federal-Provincial-Territorial Ministers and Deputy Ministers Symposium on Digital Trust and Cyber Security*.

Government of Ontario. (2026). *2026 Ontario Budget: Chapter 1B: Building Ontario's Economy*.

Government of Quebec. (2025). *Stratégie d'intégration de l'intelligence artificielle dans l'administration publique 2021–2026*.

Innovation, Science and Economic Development Canada. (2026). *Canada's National Artificial Intelligence Strategy: AI for All*.

Innovation, Science and Economic Development Canada. (2026). *Canadian Sovereign AI Compute Strategy*.

Innovation, Science and Economic Development Canada. 2026). *AI Sovereign Compute Infrastructure Program*.

References

Innovation, Science and Economic Development Canada. (2026). *Government of Canada Supports Canadian Companies Using AI to Transform Industries and Create Jobs*.

Office of the Privacy Commissioner of Canada. (2026). *Privacy and Artificial Intelligence*.

Office of the Privacy Commissioner of Canada. (2023). *Principles for Responsible, Trustworthy and Privacy-Protective Generative AI Technologies*.

Office of the Information and Privacy Commissioner of Alberta. (2025). *Framework Governing the Use of Artificial Intelligence in Alberta*.

Treasury Board of Canada Secretariat. (2026). *Guide on the Use of Generative Artificial Intelligence*.

Treasury Board of Canada Secretariat. (2025). *AI Strategy for the Federal Public Service 2025–2027: Overview*.

ACKNOWLEDGMENTS

Authors

Lucie Vignola is a senior Government of Canada executive and Chief Strategy Officer with the Institute for Citizen-Centred Service.

Yannick Newton is a Government of Canada executive and Director of Intergovernmental Cooperation with the Institute for Citizen-Centred Service.

Series Editors

This policy brief series was edited by **Liam Whittington** and **Jamie M. Thomas**.

Project Partners

Forum of Federations
The Global Network on Federalism and Devolved Governance

Publius
THE JOURNAL OF FEDERALISM

The Les Aspin Center
FOR GOVERNMENT
MARQUETTE UNIVERSITY

JAMES MADISON CHARITABLE TRUST | FOR THE STUDY OF FEDERAL SYSTEMS

Institutional Partners

This publication was made possible through the financial contributions of the institutional partners of the Forum of Federations.

Bundesministerium des Innern
Germany
Federal Ministry of the Interior

Pakistan
Senate of Pakistan

Ethiopia
House of Federation

Global Affairs Canada | Affaires mondiales Canada
Canada
Global Affairs Canada

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Switzerland
Swiss Agency for Development and Cooperation



Forum of Federations

The Global Network on Federalism and Devolved Governance



ADDRESS

75 Albert Street, Suite 411
Ottawa, ON K1P 5E7
Canada

WEBSITE

www.forumfed.org

EMAIL

forum@forumfed.org