



Canadian Shield
Institute

Foundations of Digital Sovereignty
Chapter 6 - June 2026

Procuring Sovereignty in the Cloud

Contents

Overview	1
Introduction	3
What is “Sovereign” Cloud and Compute?	4
Government as Anchor Customer	5
Level 1: No Sovereignty	7
Level 2: No Extraterritorial Access	9
Level 3: Canadian Jurisdiction	11
Level 4: Publicly Anchored	12
Conclusion and Solutions	13
References	14

Contact:

Canadian Shield Institute
150 King St. West,
Toronto, Ontario, CA

canadianshieldinstitute.ca
info@canadianshieldinstitute.ca

Authors:

Vass Bednar
James McLeod
David Corbett
Emily Osborne
Kaylie Tiessen
Matthew da Mota

Photography:

James McLeod
Patrick Tomasso
Gene Dizon

Overview

Canada doesn't need to build sovereign cloud capacity overnight, but we need a strategy for greater sovereign control and governance over cloud infrastructure. This chapter argues that government procurement is one of the most powerful tools Canada has for advancing digital sovereignty, and proposes a four-tier framework for categorizing government cloud use cases by the level of sovereign control required.

Key Takeaways

- 1 Cloud sovereignty is not a binary — it is a spectrum. The chapter proposes four levels of cloud procurement, each appropriate for different government use cases and data sensitivities:

Level 1 — No Sovereignty: Any cloud service provider may qualify. Data localization and encryption offer some protection, but foreign access risks remain. This is essentially the status quo.

Level 2 — No Extraterritorial Access: Only providers that cannot be compelled to hand over data to foreign governments qualify. This excludes American and Chinese hyperscalers subject to the CLOUD Act or equivalent legislation.

Level 3 — Canadian Jurisdiction: Data must remain exclusively under Canadian jurisdiction and on Canadian soil, handled only by wholly Canadian-owned and operated providers.

Level 4 — Publicly Anchored: The most sensitive workloads would run on government-anchored infrastructure — likely through a publicly anchored service delivery entity.

2

The federal government's data and computing needs are enormous, spanning everything from the Canada Revenue Agency to national defence. Procurement policy can use that scale to create anchor demand for Canadian cloud providers and help them grow.

3

Currently, ThinkOn is the only Canadian cloud provider pre-approved for federal use — but a Shared Services Canada RFI identified 32 Canadian suppliers with the potential to qualify.¹

4

The U.S. has explicitly listed efforts to diversify away from American hyperscalers as a trade irritant, and the 2025 U.S. National Security Strategy expressed a preference for sole-source contracts with American technology platforms. Diversifying will carry geopolitical costs — but the chapter argues they are worth bearing.

5

Government-anchored cloud capacity represents the most secure option for the most sensitive data, and could also act as a competitive force to discipline pricing across the broader market.

Canada's sovereign cloud capacity can also embed Canadian standards, data strategy and intellectual property governance considerations. Rather than an all-or-nothing approach, the framework gives the government a practical roadmap for shifting workloads toward Canadian domestic cloud capacity over time.

Introduction

As Canada works to fortify our sovereignty and resilience in a volatile world, the enormity of the challenge can be overwhelming.

As we have already seen in previous chapters of *Foundations of Digital Sovereignty*, Canada urgently needs a governance strategy for the digital economy.

We have surrendered governance of the digital realm, which means that Canadians are subject to exploitation and manipulation online, while foreign multinationals reap the economic rewards.

Canada must assert governance and strategic control over data, intellectual property and technical standards.

At the same time, Canada needs to secure our cloud infrastructure from foreign interference and coercive control. The good news is that Canada has an enormously powerful tool that can advance all of these objectives at once: procurement.

The federal government has immense data and compute needs—everything from the data processing needs of the Canada Revenue Agency to the Department of Fisheries and Oceans studying Atlantic lobster populations. By employing a procurement strategy that prioritizes sovereign control of Canadian government data and workloads, we can develop capacity and embed Canadian digital governance in a network of homegrown suppliers.



What is “Sovereign” Cloud and Compute?

The idea of a sovereign cloud tends to arise as a reaction to a clear-eyed assessment of the status quo in Canada.

Today, foreign companies dominate the Canadian cloud market at every level, and the American government has legal avenues to access most data stored in cloud infrastructure sited on Canadian soil.

As we have already seen, Canada is falling short on governing the data, the intellectual property, and the technical standards that undergird our digital systems.

The natural urge is to solve the problem by building a sovereign cloud alternative. But as we will see in this chapter, it’s much easier to define sovereign cloud in the negative — that is, we can clearly articulate all the ways that our digital infrastructure is insufficiently sovereign, but it’s much more difficult to describe what a truly sovereign cloud might actually look like.

Sovereign cloud is a system that promotes Canada’s ability to control and govern our data. A sovereign cloud system is not subject to risks of foreign interference, or at least takes steps to substantially reduce those risks. While it is almost certainly true that sovereign cloud capacity will require compute and data storage located on Canadian soil, as we have already seen, data localization is not nearly enough.

Cloud sovereignty is not a binary. Sovereign control is a gradient, where all levels of government can work to achieve higher levels of security and self-determination over Canada’s data and systems.

Due to the interconnected nature of digital infrastructure, achieving complete data sovereignty would be incredibly complicated and likely prohibitively expensive. The Government of Canada has gone as far as to call it impossible.² That being said, the current state of affairs is clearly inadequate. Strengthening Canada’s digital sovereignty is essential.

Government as Anchor Customer

Ultimately, the overarching vision we are articulating in *Foundations of Digital Sovereignty* is a future where Canada's digital economy is governed in line with Canadian values, and geared towards driving Canadian economic prosperity. The solution is not to attempt to switch all government data and computing to sovereign alternatives, but rather to determine which use cases require sovereign capacity and to what degree.

Each government cloud use case would fall into one of the following categories:

- **Level 1 - No sovereignty:** Any Cloud Service Provider (CSP) may qualify. Government cloud contracts could contain contractual language about CSPs working to prevent foreign access, and the government could pursue technical protections like encryption and data localization. However, the government understands that major risks to Canadian sovereignty are still present at this level.
- **Level 2 - No foreign access:** Information cannot be handled by any CSP subject to legislation or other channels that would grant foreign governments access to Canadian data. Only CSPs based in a country without these channels may qualify.
- **Level 3 - Canadian jurisdiction:** Information must always remain exclusively under Canadian jurisdiction and on Canadian soil. Only Canadian-owned and operated CSPs may qualify.
- **Level 4 - Publicly Anchored:** Information must remain under the exclusive control of the Canadian government. Only publicly anchored cloud capacity is to be used.

As we have articulated in Chapters 2–4, any meaningful governance of the digital economy will involve new institutions and strategies for capturing value from intellectual property and data, and embedding technical standards that strategically position Canadian companies for success.

As the Government of Canada develops a plan to expand Canada’s cloud capacity, we can embed Canadian technical standards, intellectual property, and linkages to a national data trust.

These requirements build on early signals from the Government of Canada about what digital sovereignty might look like in practice. Both the Treasury Board and Shared Services Canada have published documents that explore the topic.³

These documents suggested the importance of technical controls and the need for CSPs to be beyond the grasp of problematic extraterritorial legislation—two requirements that have been synthesized into the proposed framework.



Level 1: No Sovereignty

For use cases deemed to require little protection from foreign interference, government will continue to procure under the status quo.

Data localization and strong encryption, along with requirements for customer-held keys or key escrow, will improve protection, but they don't create Canadian cloud sovereignty when the underlying provider is subject to other international laws. Procurement will include competition between both foreign and domestic providers.

Benefits of Level 1

Continuing to procure from the American hyperscalers is arguably the cheapest option available. These companies benefit from the scale of their operations — it's why they are called hyperscalers in the first place.

The largest players are often able to price their products more competitively, or they bundle them with their other products at other layers of the digital stack. American hyperscalers already have the capacity to meet many of the government's needs.

Risks of Level 1

The most glaring risk posed by Level 1 reliance on incumbent hyperscaler CSPs is the channels for foreign access and interference that we explored in Chapter 5 of *Foundations of Digital Sovereignty*—namely, U.S. government access through the CLOUD Act and FISA.

Reliance on a few hyperscalers also introduces market concentration risks including more fragility in the market, exemplified by the October 2025 AWS outage which knocked out cloud services worldwide.⁴

Level 2: No Extraterritorial Access

CSPs who can provide clear and credible assurances that data is not subject to extraterritorial access channels would be classified as Level 2.

Level 2 requirements will be closely aligned with requirements outlined in an August 2025 Request for Information issued by Shared Services Canada which sought to understand domestic capacity for a fully sovereign public cloud solution.⁵ Data is still subject to the laws of other countries but protection is a bit more rigorous.

In practice, the federal government would maintain a registry of pre-approved CSPs that qualify for Level 2 procurement. CSPs would qualify as long as they cannot be compelled to turn over Canadian information to foreign governments, without the appropriate Canadian judicial oversight.

Benefits of Level 2

Moving data to Level 2 would reduce the risk of access by foreign governments, even if it would not fully eliminate that risk. Moving some government data to Level 2 would also increase resilience through

diversification. France-based OVHcloud and several European providers can already meet Level 2 use case needs.⁶

Risks of Level 2

Inevitably, Level 2 procurement, and all higher levels of cloud sovereignty, creates substantial risk of antagonizing the U.S. The United States National Security Strategy clearly lays out the U.S. government's preference for sole-source contracts for American technology platforms, especially when dealing with "dependent" nations.⁷ Indeed, the U.S. has listed attempts to diversify away from American hyperscalers as a trade irritant.⁸

There will also be some risk of foreign control in Level 2 cloud and compute. It is theoretically possible that any foreign government could pass legislation that undermines Canada's digital sovereignty.

Moving data out of the control of American hyperscalers may also prove to be difficult, due to an intentional lack of interoperability between cloud services, limited transparency and high egress fees.⁹

Level 3: Canadian Jurisdiction

There are some use cases where there are clear reasons to limit foreign control over cloud infrastructure.

For those use cases, cloud service procurement from Canadian CSPs would be required. This level would require a clear and actionable definition of what counts as a Canadian CSP, and which ones are eligible.

Key considerations would include company ownership, control and the location of incorporation. Only companies that are wholly owned and operated in Canada should qualify. There is clear, emerging capacity in Canada and a number of CSPs would qualify under this level.

ThinkOn is currently the only Canadian CSP pre-approved for federal use but others will follow. Shared Services Canada's "What We Heard" report identified 32 suppliers that could qualify under a similar criteria, and demonstrate a willingness to broaden capacity and diversity of supply.¹⁰

There may also be a need to exclude Canadian companies with a substantial presence in the U.S. from Level 3 such as Bell Canada Enterprises Inc. due to the nature and coverage of the U.S. CLOUD Act.¹¹

Benefits of Level 3

At Level 3, cloud services begin to look meaningfully sovereign — ensuring that government information always remains under the control of Canadian CSPs and on Canadian soil, minimizing the risks of foreign involvement.

Critical digital infrastructure would also be less exposed to potential threats, and diversifying cloud procurement through this strategy would address the risks posed by market concentration. If properly executed, procurement can act as a catalyst for increasing private sector capacity for sovereign cloud services. The increased sovereign cloud capacity would further provide more options for Canadian citizens and private sector firms who are interested in reducing their dependence on the hyperscalers.

Risks of Level 3

Foreign access to Canadian data may still pose a risk depending on how procurement requirements are structured. Further, if big Canadian enterprises are allowed to qualify, it is worth interrogating whether we feel comfortable swapping a foreign oligopoly for a domestic one.

If we aren't, we ought to consider methods that ensure procurement channels remain accessible to SMEs.

Risks of antagonizing the U.S. are similar to those associated with Level 2, but the case for weathering the potential American pushback is even stronger, given it means we are creating the space for Canadian domestic companies to scale. Similar to Level 2, there are also risks that the hyperscalers may make it difficult to transfer data or contracts away from them.

Procurement from Canadian CSPs however doesn't remove all reliance on foreign

firms or infrastructure, given the interconnected nature of the digital stack. It would be very challenging for Canada to own every layer of the digital stack or mitigate every supply chain resilience concern.¹²

Network connectivity, which is essential for supporting cloud computing, is dependent on U.S. firms and infrastructure.

A significant portion of Canadian electronic communications are routed through the U.S. via boomerang routes, which then creates a risk for U.S. surveillance of government or firm-level information, which includes sensitive IP-related information.¹³

Level 4: Publicly Anchored

Theoretically, the most secure and sovereign approach to cloud capacity would be for the government to own and operate cloud infrastructure directly.

This approach would be appropriate for most sensitive types of government information. Level 4 protection would require the government to invest in building and maintaining public-anchored cloud capacity. We will explore these ideas with more detail in Chapter 8.

The Government of Canada already has the internal capacity for storing its most sensitive data—just not through cloud computing. Because of the benefits offered by the cloud, and the government’s own cloud-first policy,¹⁴ there is a strong argument in favour of expanding this internal capacity to include cloud too.

Benefits of Level 4

Level 4 guarantees that cloud infrastructure is exclusively subject to Canadian government control and reduces the potential for any foreign interference to the greatest extent possible.

The Treasury Board’s own white paper states that the only way to maintain legal control over Canadian data is when the GC “delivers services itself or when it works with providers that operate entirely under Canadian jurisdiction.”¹⁵

A public cloud option can also prevent swapping one oligopoly for another. It can act as a competitive force, disciplining prices and practices in the market more broadly.

Risks of Level 4

Level 4 risks include price, talent attraction and retention, and public backlash. Level 4 is likely to be the most expensive option for the government. Historically speaking, the government has had difficulty attracting and retaining the digital talent needed for such initiatives.¹⁶ This risk could be mitigated by implementing through a Crown corporation or other models.

Environmental and societal impacts will need to be mitigated as much as possible in order to avoid politicizing building a government owned sovereign cloud.

Conclusion

As we have already discussed at length in the previous chapters of *Foundations of Digital Sovereignty*, physical infrastructure isn't the most important dimension of our digital systems. Economic value and social impact come primarily from flows of data and from platform software design choices. Governing the digital layer is more meaningful for capturing value and shaping the technology we use, and focusing on where the servers are physically sited misses this reality.

However, a comprehensive approach to digital sovereignty will include more homegrown Canadian companies operating within a framework of Canadian technical standards and laws.

As we have seen, Canadian data is currently vulnerable to foreign access and control. Our current approach leaves us structurally dependent on foreign hyperscalers subject to legal regimes and geopolitical considerations that Canada does not control.

Through the use of strategic procurement, the Government of Canada can level-up domestic private sector cloud and compute capacity, while also developing greater in-house expertise in the technical realities of digital infrastructure.

Building a sovereign cloud is not simply about racks of servers on the outskirts of a Canadian city. It is about embedding Canadian strategic governance in the tech stack. Asserting our sovereignty will be expensive and challenging, but it is an investment worth making.

Solutions

Canada's structural dependence on foreign hyperscalers will not resolve itself — but strategic procurement can begin to shift the balance. To assert sovereign control over government data and build domestic cloud capacity, the Government of Canada should:

- 1 **Adopt the four-level procurement framework**, mapping all government cloud workloads to the appropriate sovereignty level based on their sensitivity, security classification, and public interest requirements.
- 2 **Establish and maintain a registry of pre-approved Canadian CSPs eligible for Level 2 and Level 3 procurement**, with clear and enforceable criteria for ownership, incorporation, and freedom from foreign legal jurisdiction.
- 3 **Embed technical protections** — including end-to-end encryption with customer-held keys — and foreign access disclosure obligations into all procurement contracts, including those with hyperscalers at Level 1.
- 4 **Use government procurement as an anchor to grow domestic cloud capacity**, ensuring contract structures are accessible to Canadian SMEs and do not simply replace a foreign oligopoly with a domestic one.
- 5 **Begin developing government-owned cloud capacity for the most sensitive workloads**, with a crown corporation model as the vehicle for building the institutional permanence and governance depth that Level 4 sovereignty needs.

References

- 1 Shared Services Canada, “RFI Sovereign Public Cloud Capabilities: What we heard report,” Government of Canada, November 19, 2025, <https://canadabuy.ca/en/tender-opportunities/tender-notice/cb-416-17296820>.
- 2 Government of Canada, “Digital Sovereignty: A Framework to improve digital readiness of the Government of Canada,” last modified November 12, 2025, <https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/digital-sovereignty/digital-sovereignty-framework-improve-digital-readiness.html#toc4>.
- 3 Government of Canada, “Digital Sovereignty: A Framework,” Shared Services Canada, *Request for Information - Sovereign Public Cloud Capability*, Solicitation no. CS-IAAS-2025, August 13, 2025, <https://www.merx.com/public/supplier/solicitations/notice/22784981390/abstract>; Treasury Board of Canada Secretariat, “Government of Canada white paper: data sovereignty and public cloud,” Government of Canada, June 25, 2018, <https://publications.gc.ca/site/eng/9.858956/publication.html>.
- 4 Dan Milmo and Graeme Wearden, “Amazon Web Services outage shows internet users ‘at mercy’ of too few providers, experts say,” *The Guardian*, October 20, 2025, <https://www.theguardian.com/technology/2025/oct/20/amazon-web-services-aws-outage-hits-dozens-websites-apps>.
- 5 Shared Services Canada, *Sovereign Public Cloud Capability*.
- 6 “European cloud computing platforms,” European Alternatives, accessed February 6, 2026, <https://european-alternatives.eu/category/cloud-computing-platforms>.
- 7 Matthew da Mota and Emily Osborne, “‘Sole-source’ clause in new U.S. National Security Strategy runs roughshod over Canadian sovereignty,” *Financial Post*, December 22, 2025, <https://financialpost.com/news/economy/new-us-nss-clause-roughshod-canadian-sovereignty>.
- 8 Raphael Satter and Alexandra Alper, “Exclusive: US orders diplomats to fight data sovereignty initiatives,” *Reuters*, February 25, 2026, <https://www.reuters.com/sustainability/boards-policy-regulation/us-orders-diplomats-fight-data-sovereignty-initiatives-2026-02-25/>.
- 9 Songrim Koo and Connor Hogg, “Competition in the Provision of Cloud Computing Services,” *OECD Roundtables on Competition Policy Papers*, no. 323 (2025), https://www.oecd.org/content/dam/oecd/en/publications/reports/2025/05/competition-in-the-provision-of-cloud-computing-services_f42582ad/595859c5-en.pdf; CMA, “Cloud Services Market Investigation: Summary of Final Decision,” July 31, 2025, https://assets.publishing.service.gov.uk/media/688b20e6ff8c05468cb7b120/summary_of_final_decision.pdf.

10 Shared Services Canada, “What we heard report.”

11 Michael Geist, “The catch-22 of Canadian digital sovereignty,” *The Globe and Mail*, December 10, 2025, <https://www.theglobeandmail.com/business/commentary/article-the-catch-22-of-canadian-digital-sovereignty/>.

12 John Ruffolo and Peter Shi, “Canada’s Digital Sovereignty: From Buzzword to Blueprint,” *Stories by John Ruffolo on Medium* (blog), December 1, 2025, <https://johnruffolo.substack.com/p/canadas-digital-sovereignty-from>; Madison McLauchlan, “Canada hopes to build a sovereign cloud to counter US dominance. It won’t be easy,” *Betakit*, September 25, 2025, <https://betakit.com/canadian-sovereign-cloud-evan-solomon-all-in/>.

13 Andrew Clement, “Canadian Network Sovereignty: A Strategy for Twenty-First-Century National Infrastructure Building,” CIGI, March 26, 2018, <https://www.cigionline.org/articles/canadian-network-sovereignty/>.

14 Treasury Board of Canada Secretariat, “Government of Canada white paper.”

15 Government of Canada, “Digital Sovereignty: A Framework.”

16 Government of Canada, “Digital Sovereignty: A Framework,” 2025.