

U.S. Federal Cloud Strategy and Governance (Adapted from Canada's GGCL)

Overview: The United States pioneered a shift to cloud computing in government with its “**Cloud First**” policy in 2010, and later the more nuanced “**Cloud Smart**” strategy in 2019¹. Where Canada's GGCL (Guidelines for Government Cloud Use) emphasizes data residency (Protected B data, sovereign cloud initiatives) due to reliance on foreign providers, the U.S. approach has centered on **broad cloud adoption through standardized security frameworks (e.g. FedRAMP)** and modernization guidance, **with most U.S. federal data already hosted by domestic cloud vendors**. Below we detail the U.S. policies, security compliance regimes (FISMA/NIST, FedRAMP, TIC 3.0), key agencies and programs (OMB's Cloud Smart, GSA's FedRAMP, DoD's JWCC), and recent developments (laws, executive orders) shaping American public-sector cloud use – with comparisons to Canada's practices where relevant.

U.S. Cloud Policies: From “Cloud First” to “Cloud Smart”

The U.S. federal cloud journey began with the **Cloud First** policy introduced under Federal CIO Vivek Kundra in 2011. Cloud First mandated that agencies **migrate suitable IT systems to cloud solutions whenever secure and economical**, aiming to shut down hundreds of duplicative data centers and save costs². However, Cloud First offered broad authority without detailed how-to guidance. Many agencies struggled with ad-hoc migrations that revealed challenges: unanticipated **higher costs** (e.g. data egress fees, idle capacity)³, **security concerns** (loss of direct control)⁴, **legacy apps not cloud-ready**, and risk of **vendor lock-in** with single providers⁵. In practice, Cloud First led to uneven progress – some early

¹<https://www.cyberdefensemagazine.com/four-years-and-a-pandemic-later-have-agencies-become-cloud-smart/>

²<https://www.cyberdefensemagazine.com/four-years-and-a-pandemic-later-have-agencies-become-cloud-smart/>

³<https://www.cyberdefensemagazine.com/four-years-and-a-pandemic-later-have-agencies-become-cloud-smart/>

⁴<https://www.cyberdefensemagazine.com/four-years-and-a-pandemic-later-have-agencies-become-cloud-smart/>

⁵<https://www.cyberdefensemagazine.com/four-years-and-a-pandemic-later-have-agencies-become-cloud-smart/>

adopter agencies moved email and collaboration to commercial clouds, but others lagged or encountered cost overruns.

Cloud Smart (2019): Learning from those lessons, OMB replaced Cloud First with the **Federal Cloud Computing Strategy: Cloud Smart** in June 2019^{6 7}. Cloud Smart delivers more nuanced, flexible guidance, built on three pillars: **security, procurement, and workforce**^{8 9}. Instead of an indiscriminate “move everything” approach, it emphasizes agencies should **evaluate mission needs and application readiness** to choose the right model (public, private, hybrid, multi-cloud)¹⁰. Key tenets of Cloud Smart include:

- **Risk-based Security & Shared Responsibility:** Agencies must adopt a “defense-in-depth” approach for cloud security, protecting data at multiple layers (not just the network perimeter)¹¹. Cloud Smart points to updated programs like **FedRAMP** (cloud security authorizations) and **TIC 3.0** (Trusted Internet Connections 3.0) that accommodate modern cloud architectures^{12 13}. It encourages use of **Zero Trust** principles (assuming no implicit trust even inside networks) and continuous monitoring of cloud assets. (By contrast, Canada’s GGCL similarly stresses rigorous compliance but focuses on data localization – the US places more weight on framework-based risk management since most providers are domestic.)
- **Smarter Procurement:** Cloud Smart calls for buying cloud based on actual **consumption and service needs** rather than bulk capacity¹⁴. Agencies are urged to avoid vendor lock-in by using **best-in-class contracts** and negotiating strong **Service**

⁶<https://cloud.cio.gov/strategy/>

⁷<https://cloud.cio.gov/strategy/>

⁸<https://cloud.cio.gov/strategy/>

⁹<https://www.cyberdefensemagazine.com/four-years-and-a-pandemic-later-have-agencies-become-cloud-smart/>

¹⁰<https://www.cyberdefensemagazine.com/four-years-and-a-pandemic-later-have-agencies-become-cloud-smart/>

¹¹<https://cloud.cio.gov/strategy/>

¹²<https://cloud.cio.gov/strategy/>

¹³<https://cloud.cio.gov/strategy/>

¹⁴<https://www.cyberdefensemagazine.com/four-years-and-a-pandemic-later-have-agencies-become-cloud-smart/>

Level Agreements (SLAs) with clear performance metrics and remedies^{15 16}.

(Notably, a 2024 GAO review found many agencies still lacked standardized cloud SLAs¹⁷ – OMB’s policy was sound, but execution has been uneven. The Canadian approach similarly emphasizes careful contracting, though Canada’s focus has been on requiring cloud providers to store data in Canada and potentially exit arrangements if sovereignty is at risk, whereas U.S. contracts focus on uptime, security compliance, and cost control.)

- **Workforce & Skills:** Recognizing that adopting cloud is as much about people as tech, Cloud Smart pushes agencies to **train IT staff in cloud architectures, DevSecOps, and modern procurement**^{18 19}. It calls for upskilling in areas like agile development, cloud security management, and multi-vendor management. Both U.S. and Canadian governments face cloud talent gaps; Cloud Smart and Canada’s digital academy initiatives share the goal of equipping workers to manage cloud services effectively.

Cloud Smart was a direct outcome of the 2017 Executive Order 13800 on cybersecurity, which mandated an updated cloud strategy²⁰. It effectively aligned U.S. policy with what Canada codified in its 2018 cloud-first directive – that is, embrace cloud but **“use the right cloud for the right workload”** instead of one-size-fits-all. For instance, Cloud Smart explicitly says not everything belongs in a public cloud and hybrid solutions can be optimal²¹, whereas Canada’s early cloud-first policy also allowed exceptions for highly sensitive systems (now Canada even reserves “Protected C” classified data for on-premise only). In practice, U.S. agencies have taken a mix of approaches: some moved aggressively to commercial clouds (e.g. USDA’s farmers benefit programs), others built **private government clouds** or used **community clouds** (e.g. the intelligence community’s IC GovCloud). Cloud Smart empowers each agency CIO to pursue what makes sense while following government-wide best practices.

¹⁵<https://www.gao.gov/products/gao-24-106137>

¹⁶<https://www.gao.gov/products/gao-24-106137>

¹⁷<https://www.gao.gov/products/gao-24-106137>

¹⁸<https://cloud.cio.gov/strategy/>

¹⁹<https://www.cyberdefensemagazine.com/four-years-and-a-pandemic-later-have-agencies-become-cloud-smart/>

²⁰<https://cloud.cio.gov/strategy/>

²¹<https://www.cyberdefensemagazine.com/four-years-and-a-pandemic-later-have-agencies-become-cloud-smart/>

Governance: The **Office of Management and Budget (OMB)** oversees compliance with Cloud Smart, tracking progress via CIO Council initiatives and the **FITARA Scorecard** (Congress’s biannual agency IT assessment). In fact, a new “cloud adoption” scoring area was added to the FITARA Scorecard in 2023, which initially caused several agencies’ grades to drop – indicating many had not fully implemented Cloud Smart tenets^{22 23}. This public grading has spurred lagging agencies to formalize cloud policies (e.g. issuing internal cloud procurement guidelines with SLA templates, as GAO recommended)^{24 25}.

Meanwhile, OMB continues to release cloud-related memoranda. For example, OMB’s **M-21-05 (2020)** set data center closure targets through 2025 (tying into cloud migration savings), and **M-22-09 (2022)** required agencies to meet specific Zero Trust security goals by 2024 – many of which involve cloud-based solutions for identity, logging, and threat detection. President Biden’s **Executive Order 14028 (2021)** on cybersecurity also explicitly calls for **accelerating movement to secure cloud services and zero-trust frameworks** for all agencies^{26 27}. In summary, the U.S. policy environment strongly encourages cloud adoption, but with an evolving emphasis on *how* to do so securely and efficiently, rather than just *how much*. (Canada’s evolving policy mirrors this: after its initial “Cloud First” push, the Canadian Treasury Board Secretariat in 2022–2023 introduced more guidance on workload assessment, application readiness, and even allowed some repatriation if cloud isn’t cost-effective – a parallel to the U.S. realization that cloud is “**not a destination**” but an operating model²⁸.)

Security and Compliance Frameworks: FISMA, FedRAMP, and TIC 3.0

Underpinning the U.S. government’s cloud adoption is a robust security and compliance framework set by law and standards. The **Federal Information Security Modernization Act (FISMA)** requires every federal system – including cloud-hosted systems – to implement a risk-based security program aligned with **NIST** guidelines. Key elements include:

²²<https://www.cyberdefensemagazine.com/a-cloud-reality-check-for-federal-agencies/>

²³<https://www.cyberdefensemagazine.com/a-cloud-reality-check-for-federal-agencies/>

²⁴<https://www.gao.gov/products/gao-24-106137>

²⁵<https://www.gao.gov/products/gao-24-106137>

²⁶<https://cloud.cio.gov/strategy/>

²⁷<https://cloud.cio.gov/strategy/>

²⁸<https://www.cyberdefensemagazine.com/four-years-and-a-pandemic-later-have-agencies-become-cloud-smart/>

- **NIST 800-53 Controls & FIPS 199 Categories:** U.S. agencies categorize their systems as Low, Moderate, or High impact for **confidentiality, integrity, and availability**, per FIPS 199^{29 30} – similar to how Canada designates information up to Protected B/C. For each impact level, NIST SP 800-53 provides a baseline set of security controls. A cloud system handling, say, sensitive PII or financial data would be Moderate impact, requiring ~300 controls; health or law enforcement data might be High (more controls). This categorization feeds directly into the **FedRAMP** program.
- **FedRAMP (Federal Risk and Authorization Management Program):** FedRAMP is a centralized cloud security authorization process launched in 2011 and now required by law³¹. **Cloud service providers (CSPs) must undergo an independent assessment of their security controls (based on NIST 800-53) and obtain a FedRAMP ATO (Authority to Operate) at a defined impact level** before U.S. agencies can use them. FedRAMP offers three standardized baselines:
 - **Low Impact** – For minor applications (public data or low-sensitivity SaaS). E.g. a project management tool with no sensitive data may be FedRAMP Low³².
 - **Moderate Impact** – Covers ~80% of FedRAMP approvals³³. This is the baseline for most federal systems containing personally identifiable information, routine mission data, etc. (Close analog: Canada’s Protected B data). E.g. a cloud email service for unclassified but sensitive email must be FedRAMP Moderate.
 - **High Impact** – For the government’s most sensitive unclassified data (health records, law enforcement, emergency services, financial systems)³⁴. Only a subset of CSPs have FedRAMP High ATOs, often using separate U.S. GovCloud regions and U.S.-citizen personnel for added assurance. (There is no public FedRAMP for classified – DoD/IC handle Secret/Top Secret clouds separately, akin to Canada keeping classified off public cloud.)

²⁹<https://www.fedramp.gov/archive/2017-11-16-understanding-baselines-and-impact-levels/>

³⁰<https://www.fedramp.gov/archive/2017-11-16-understanding-baselines-and-impact-levels/>

³¹<https://www.fedramp.gov/archive/2023-01-11-announces-passing-fedramp-auth-act/>

³²<https://www.fedramp.gov/archive/2017-11-16-understanding-baselines-and-impact-levels/>

³³<https://www.fedramp.gov/archive/2017-11-16-understanding-baselines-and-impact-levels/>

³⁴<https://www.fedramp.gov/archive/2017-11-16-understanding-baselines-and-impact-levels/>

- A FedRAMP authorization involves rigorous documentation (hundreds of security controls), penetration testing, continuous monitoring, and annual reassessment. Critically, once a cloud service is FedRAMP-authorized at a given level, **any agency can reuse that authorization** rather than repeating the full assessment. This reuse was a major rationale for FedRAMP's creation – to prevent each of the 100+ agencies from separately auditing Microsoft Azure, Amazon AWS, etc. By 2022–2023, FedRAMP had facilitated **4,500 reuse instances of cloud services across agencies in a single year**³⁵, showing a dramatic increase in cross-agency trust of cloud security. (In Canada, an analogous process exists in the form of the GC Cloud Security Risk Management framework, but it is less centralized; Canada often leverages FedRAMP reports when assessing major cloud services for Protected B, reflecting the maturity of the U.S. regime.)
- FedRAMP is overseen by a Joint Authorization Board (JAB) of top CIOs (from DoD, DHS, GSA) who can grant a **provisional ATO** for government-wide use, or agencies can grant their own FedRAMP ATO which others may reuse. In January 2023, the **FedRAMP Authorization Act** elevated this program into law, mandating stronger reciprocity (agencies must check FedRAMP before assessing a cloud on their own) and establishing a federal Secure Cloud Advisory Committee with industry and agency members to improve FedRAMP processes^{36 37}. This legislative backing is similar to Canada's recent push to formalize cloud risk management and advisory bodies (the U.S. move came after a decade of FedRAMP operations, whereas Canada's cloud security program is newer and still evolving alongside FedRAMP's model).
- **Trusted Internet Connections (TIC) 3.0:** One challenge in early U.S. cloud adoption was the **TIC** policy (2007) that forced agency traffic through a limited number of approved access points for security monitoring (the EINSTEIN intrusion detection system)³⁸. Traditional TIC 1.0/2.0 gateways didn't fit well with direct SaaS or commercial cloud access, causing latency and design issues. In response, **TIC 3.0 (2019)** revamped the model to be use-case based and allow alternative security architectures for cloud (e.g. enhanced endpoint security and cloud-native logging in lieu of all traffic backhauled through a physical TIC)^{39 40}. DHS's Cybersecurity and

³⁵<https://www.fedramp.gov/archive/2023-01-11-announces-passing-fedramp-auth-act/>

³⁶<https://www.fedramp.gov/archive/2023-01-11-announces-passing-fedramp-auth-act/>

³⁷<https://www.fedramp.gov/archive/2023-01-11-announces-passing-fedramp-auth-act/>

³⁸<https://cloud.cio.gov/strategy/>

³⁹<https://cloud.cio.gov/strategy/>

⁴⁰<https://cloud.cio.gov/strategy/>

Infrastructure Security Agency (CISA) published reference architectures showing how agencies can meet TIC objectives (like centralized threat monitoring via EINSTEIN) even with distributed cloud services^{41 42}. Essentially, TIC 3.0 aligns network security with Cloud Smart: it permits **direct cloud access with proper zero-trust controls and continuous diagnostics (CDM)** instead of forcing everything through on-prem hubs. Canada faces a similar issue with its own perimeter security; the U.S. pivot with TIC 3.0 has informed Canada's approach of using modern cloud security brokers and monitoring rather than a single pipe – both countries recognize that legacy perimeter-only defenses must evolve for cloud.

- **Continuous Monitoring & Incident Response:** Both U.S. and Canadian frameworks stress ongoing oversight of cloud assets. Under FedRAMP, CSPs must provide agencies with continuous monitoring reports (regular scans, audit logs) and notify of incidents. OMB M-21-31 (Aug 2021) specifically required agencies to log authoritative data on all cloud activity and suggested use of cloud-native log services to enhance detection (this was partly driven by major incidents like the SolarWinds breach). In practice, U.S. agencies are negotiating improved contractual clauses for **continuous visibility** into cloud-hosted High Value Assets – yet as GAO noted in 2024, many agencies still hadn't standardized those requirements in contracts^{43 44}. The CIO Council is now sharing sample language (e.g. stipulating on-demand access to cloud log data and on-premise copy of security logs) to enforce visibility on par with on-prem systems. (Canada's cloud contracts likewise address incident reporting and Government of Canada access to provider logs, though Canada has fewer large-scale cloud deployments so far; the U.S. lessons on visibility in multi-tenant clouds are actively informing Canadian security guidelines.)

Agency Roles: In the U.S., cloud security and compliance involve multiple authorities:

- **OMB** – sets overall policy (e.g. Cloud Smart, FISMA guidance) and adjudicates any agency implementation plans.
- **NIST** – defines the technical standards (like NIST 800-145 defining cloud characteristics, NIST 800-53 controls baseline⁴⁵, NIST 800-207 for Zero Trust, etc.) that shape agency requirements and FedRAMP standards.

⁴¹<https://cloud.cio.gov/strategy/>

⁴²<https://cloud.cio.gov/strategy/>

⁴³<https://www.gao.gov/products/gao-24-106137>

⁴⁴<https://www.gao.gov/products/gao-24-106137>

⁴⁵<https://www.fedramp.gov/archive/2017-11-16-understanding-baselines-and-impact-levels/>

- **FedRAMP PMO (within GSA)** – runs the day-to-day program (authorizations, marketplace of approved services).
- **CISA (DHS)** – leads federal cybersecurity programs like TIC and Continuous Diagnostics & Mitigation (CDM) adapted for cloud, and operates EINSTEIN sensors that now integrate with cloud environments^{46 47}.
- **Agency CIOs & CISOs** – ultimately responsible for securing their cloud deployments under FISMA. Each agency’s CIO must sign off Authority to Operate (ATO) for systems (even with FedRAMP, the agency issues the final ATO). Many agencies have established **Cloud Centers of Excellence** or cloud management offices to centralize expertise.
- **Department of Defense (DoD)** – has parallel but related frameworks: the DoD Cloud Computing Security Requirements Guide maps to FedRAMP but adds stricter controls and defines **Impact Levels 2/4/5/6** (IL6 being classified Secret) for DoD data. DoD’s approach heavily influenced JWCC and its requirements for vendors at IL5-IL6 (e.g. AWS Secret Region, Microsoft Azure Government Secret are tailored offerings to meet those needs). The DoD CIO and Defense Information Systems Agency (DISA) thus manage classified cloud approvals outside FedRAMP, but at unclassified levels, DoD also reuses FedRAMP Moderate/High for efficiency. (Similarly, Canada’s Department of National Defence keeps classified systems on-premises or in separate arrangements, while leveraging public cloud for unclassified workloads; both countries set a clear boundary that **classified info requires dedicated infrastructure** – e.g. the U.S. Intelligence Community runs the IC GovCloud via a commercial partnership, comparable in concept to Canada’s guarded “Secret Infrastructure”).

In essence, the U.S. has built a comprehensive ecosystem of policies and programs to ensure cloud services meet federal security requirements. **This reliance on standard frameworks differs from Canada’s sovereignty-centered stance:** where Canada might ask “Is our data staying in Canada’s jurisdiction?”, the U.S. asks “Is the cloud service FedRAMP certified and continuously monitored?”. Notably, **data sovereignty is less contentious for U.S. federal agencies** because the major cloud providers (AWS, Microsoft, Google, Oracle) are U.S.-based and subject to U.S. law – the government is more concerned with **supply-chain security** (keeping out foreign technology influence) than with the provider being subject to foreign jurisdiction. In fact, legislation like the CLOUD Act (2018) gives U.S. law enforcement rights to reach data held by U.S. companies overseas, whereas in Canada/EU that raised alarms. Thus Canada and Europe have pursued “sovereign cloud” solutions to avoid U.S. legal reach; the U.S. doesn’t face that issue domestically. Instead, the U.S. ensures **cloud sovereignty** in another sense: requiring that sensitive federal data is handled only in

⁴⁶<https://cloud.cio.gov/strategy/>

⁴⁷<https://cloud.cio.gov/strategy/>

FedRAMP High cloud regions on U.S. soil by U.S. personnel (for example, Department of Defense IL5 contracts stipulate U.S. citizenship for admins). So both countries care about who can access data – the U.S. implements it via FedRAMP and contract restrictions, while Canada sometimes must insist on domestic hosting or even Canadian-operated clouds (as in its recent “Cloud Sovereignty” pilots) to mitigate the dominance of foreign (American) vendors.

Cloud Deployment in Practice: Usage, Programs, and Trends

After more than a decade, U.S. federal agencies have made substantial use of cloud services, though full transformation is ongoing. As of FY2023, civilian agencies were spending an estimated **\$8 billion+ per year on cloud** (out of ~\$65 billion total federal IT spend)⁴⁸. Nearly all of the 24 major departments have migrated commodity services like email, collaboration suites, and websites to a cloud environment. For example:

- The **Department of the Treasury** consolidated 91% of its email users onto Microsoft Office 365 Government Cloud by 2022 (FedRAMP Moderate) and is closing legacy email systems.
- The **Census Bureau** used AWS cloud to securely collect and process data for the 2020 Census – an effort that earned FedRAMP High authorizations and scaled on-demand.
- **USDA** moved its farmers benefit portal to the cloud to improve uptime for users in rural areas, leveraging commercial CDN and cloud regions for better performance.

Even classified and defense workloads are embracing cloud: the **Pentagon’s JWCC** contract, awarded in Dec 2022, allows the Department of Defense to obtain cloud infrastructure and SaaS at all classification levels from multiple vendors on a common contract^{49 50}. By mid-2023, the DoD CIO directed all components to “**use JWCC as the first resort**” for any new cloud needs, to prevent siloed contracting. JWCC services are expected to be **operational by 2024** with Top Secret cloud nodes and tactical-edge deployable cloud stacks for military use^{51 52}. This mirrors a trend: specialized government community clouds. (Canada hasn’t

⁴⁸<https://www.cyberdefensemagazine.com/a-cloud-reality-check-for-federal-agencies/>

⁴⁹<https://www.nationaldefensemagazine.org/articles/2021/7/6/pentagon-cancels-jedi-program-launches-new-cloud-computing-effort>

⁵⁰<https://www.nationaldefensemagazine.org/articles/2021/7/6/pentagon-cancels-jedi-program-launches-new-cloud-computing-effort>

⁵¹<https://www.nationaldefensemagazine.org/articles/2021/7/6/pentagon-cancels-jedi-program-launches-new-cloud-computing-effort>

⁵²<https://www.nationaldefensemagazine.org/articles/2021/7/6/pentagon-cancels-jedi-program-launches-new-cloud-computing-effort>

gone to that scale for defense; its approach to national security cloud still relies on internal data centers, although there are discussions of secure community cloud for defense in future. The U.S. JWCC can be seen as roughly analogous to a hypothetical Canadian multi-vendor “Protected C cloud” – something Canada may explore as its military modernizes IT.)

Procurement Evolution: U.S. agencies historically procured cloud via GSA Schedule contracts or their own vehicles, sometimes leading to duplication and inconsistent terms. In recent years, emphasis on **government-wide acquisition contracts** and **category management** has increased. For example, GSA’s **Schedule 70** now has special SINs (Special Item Numbers) for cloud computing, and **government-wide contracts like NASA SEWP V** and **GSA Alliant 2** are commonly used for cloud services. OMB’s category management policy (2019) explicitly calls for agencies to use best-in-class contracts for cloud when possible^{53 54}. The DoD’s JWCC itself is an enterprise vehicle to prevent each military branch from contracting its own cloud separately. The **CIO Council** has also created a **Cloud Marketplace** portal to help agencies identify FedRAMP-authorized offerings and contract vehicles easily. These measures parallel Canada’s approach where Shared Services Canada offers cloud procurement instruments and a “Government of Canada Cloud Brokering” service for departments – both countries realized coordinated buying improves security and pricing.

One notable procurement shift in the U.S. is the focus on **Service Level Agreements and cost management**. As GAO reported in 2024, only 6 of 24 CFO-act agencies had fully addressed OMB’s requirement to have comprehensive SLAs for every cloud service covering performance, roles, remedies, and continuous availability⁵⁵. Moreover, cloud costs have sometimes surprised agencies (e.g. NIH found data egress fees consuming budget more than expected). Cloud Smart and subsequent guidance urge agencies to **implement cloud cost governance**, including use of tools for tracking usage and enforcing budget caps^{56 57}. The U.S. is increasingly adopting FinOps (cloud financial management) practices – similar to Canada’s concerns that pay-as-you-go cloud needs new budgeting approaches. On the positive side, agencies can achieve savings by shutting down redundant systems: e.g. the Department of Veterans Affairs retired 24 data centers after moving systems to clouds, contributing to the government having closed over **6,000 data centers by 2019** under the

⁵³<https://cloud.cio.gov/strategy/>

⁵⁴<https://cloud.cio.gov/strategy/>

⁵⁵<https://www.gao.gov/products/gao-24-106137>

⁵⁶<https://www.cyberdefensemagazine.com/a-cloud-reality-check-for-federal-agencies/>

⁵⁷<https://www.cyberdefensemagazine.com/a-cloud-reality-check-for-federal-agencies/>

Federal Data Center Optimization Initiative (well ahead of Canada's smaller-scale data center consolidation).

Data Sovereignty and Locality: While, as noted, U.S. agencies generally host data with American companies inside the U.S., there are still sovereignty-adjacent concerns: one is **state/local data** in federal clouds and **citizen privacy**. For instance, the U.S. CLOUD Act can compel providers to hand over data to law enforcement via proper legal process – federal agencies must ensure any **international data they handle (e.g. data from ally governments or global programs)** is protected by agreements. Additionally, some agencies require cloud vendors to employ **U.S. persons with security clearances** for certain sensitive operations (particularly DoD IL5/6 and IC cloud work) – a practice analogous to Canada's requirement that certain cloud support must be performed by Canadians for Protected B data.

In recent years, there have been calls in the U.S. to develop **"sovereign clouds" for allies** – for example, American CSPs offering EU-only cloud instances to satisfy European regulators. Domestically, however, the focus is on ensuring **supply chain integrity**: via the Federal Acquisition Security Council, the U.S. can exclude foreign adversary components from federal cloud systems (e.g. a ban on Chinese telecom equipment in data centers). This is somewhat inverse to Canada, which worries about U.S. suppliers; the U.S. worries about Chinese or other non-allied influence. Both countries share the goal of **trusted cloud infrastructure**, just facing different threat vectors.

Recent Developments: In addition to the FedRAMP law and JWCC already discussed, some notable U.S. moves include:

- A push for **Zero Trust by 2024**: OMB's 2022 Zero Trust Architecture Strategy (M-22-09) requires agencies to meet specific targets (e.g. encrypting all traffic, centralized identity management) for their cloud and on-prem systems. Agencies are implementing cloud-based identity platforms and Secure Access Service Edge (SASE) solutions as part of this mandate, investing TMF (Technology Modernization Fund) dollars in such upgrades. This makes cloud environments more secure and accelerates cloud adoption (since zero trust network configurations often presume cloud-native tech).
- **FITARA Scorecard Cloud Measures**: As mentioned, Congress (House Oversight Committee) added a Cloud Adoption metric in 2023. In the first assessment, only **8 agencies scored an "A" or "B"** on cloud (meaning high percentage of systems moved or optimized for cloud), while others got "C" or below^{58 59}. This public transparency creates pressure – e.g. the Department of **Energy**, which scored low partially due to lacking cloud-specific guidance, is now forming a cloud governance board and

⁵⁸<https://www.cyberdefensemagazine.com/a-cloud-reality-check-for-federal-agencies/>

⁵⁹<https://www.cyberdefensemagazine.com/a-cloud-reality-check-for-federal-agencies/>

writing the required SLA policies to boost its grade^{60 61}. Such oversight mechanisms have no direct Canadian analogue (Canada has no public scorecard, though Treasury Board monitors departments); it shows the U.S. commitment to making cloud progress measurable and accountable.

- **State and Local Alignment:** Although not part of federal GGCL, it's worth noting many U.S. states follow FedRAMP standards for their own cloud procurements (for efficiency). And the FedRAMP Authorization Act encourages reciprocal recognition of FedRAMP between U.S. federal agencies and other governments (including potentially Canada in the future). Indeed, in 2022 the U.S. and Canada announced cooperation on cloud security under the Joint Action Plan for Critical Infrastructure – exploring ways a FedRAMP authorization could simplify cloud approval in Canada and vice versa (though data residency differences remain a sticking point).

In sum, the United States has built a **comprehensive cloud governance ecosystem** that differs from Canada's GGCL emphasis but achieves similar ends: safe, cost-effective cloud adoption. The U.S. relies on **standardized frameworks (FedRAMP, NIST) and market-driven solutions** under strong central policies (Cloud Smart), whereas Canada has had to place more **sovereignty safeguards** and create bespoke "Cloud Center of Excellence" arrangements to broker U.S. providers for Canadian needs. Both nations are now converging on best practices like zero trust, multi-cloud flexibility, and workforce training. As cloud technologies continue to evolve (edge computing, AI services), the U.S. is well-positioned with its cloud-smart, risk-managed approach – agencies can choose from a rich marketplace of **~280 FedRAMP-approved services**⁶² including advanced SaaS/PaaS offerings, and have legal/governance tools in place to keep those services in check. Challenges remain (e.g. controlling costs and avoiding lock-in), but ongoing initiatives and oversight are addressing these (as GAO's recommendations are implemented⁶³). Meanwhile, Canada can draw lessons from the U.S. experience: the importance of a centralized security vetting program, the need for clear SLA and cost management policies, and the benefit of multi-vendor enterprise contracts for cloud.

Ultimately, the U.S. federal cloud strategy demonstrates how a **large government can embrace cloud at scale** – by combining **top-down policy (OMB), rigorous security standards (FedRAMP/NIST), and continuous improvement via oversight and industry engagement** – a model that influences cloud governance globally. The American context shows that cloud adoption is not simply an IT project but a sustained operational paradigm shift, requiring

⁶⁰<https://www.gao.gov/products/gao-24-106137>

⁶¹<https://www.gao.gov/products/gao-24-106137>

⁶²<https://www.fedramp.gov/archive/2023-01-11-announces-passing-fedramp-auth-act/>

⁶³<https://www.gao.gov/products/gao-24-106137>

adjustments in procurement, risk management, and culture. As both the U.S. and Canada continue on their cloud journeys, their approaches – though shaped by different sovereignty contexts – are increasingly aligned in pursuing secure, agile, and smart use of cloud to deliver public services.

64 65 66

⁶⁴<https://www.cyberdefensemagazine.com/four-years-and-a-pandemic-later-have-agencies-become-cloud-smart/>

⁶⁵<https://www.gao.gov/products/gao-24-106137>

⁶⁶<https://www.fedramp.gov/archive/2023-01-11-announces-passing-fedramp-auth-act/>