

Canada

Directive on Service and Digital

August 29, 2025

Overview

Effective April 1, 2026, the Government of Canada's [Directive on Service and Digital](#) establishes a unified framework for strengthening federal service delivery, digital governance, cybersecurity, and data stewardship. The Directive defines how departments must plan, design, and manage digital services and technology investments.

The 2026 update emphasizes integrated digital planning, enterprise platform adoption, cloud-first modernization, privacy by design, accessibility, and user-centric service delivery. It aligns departmental requirements with key Government of Canada frameworks, reinforcing secure development, responsible AI use, and improved data management practices.

Overall, the Directive ensures that digital investments support enterprise priorities and deliver measurable improvements in service performance, interoperability, and security across government.

Framework

The Directive on Service and Digital establishes a unified operating model for how federal departments govern, deliver, and secure digital services. The framework centers on integrated decision-making, enterprise level coordination, and risk-informed technology management, ensuring that digital initiatives are accountable and measurable across the Government of Canada.

The 2026 update strengthens federal governance by clarifying roles, responsibilities, and oversight mechanisms tied to digital investments, service performance, and technology operations. It introduces tighter alignment between departmental planning and government-wide priorities, expands requirements for monitoring and reporting, and reinforces the use of common enterprise solutions to reduce fragmentation.

Framework components include:

- **Integrated Digital Governance**
 - Establishes clear decision-making and oversight structures for digital investments, ensuring alignment with enterprise priorities and measurable outcomes.
- **Enterprise Coordination Mechanisms**
 - Requires departments to use shared platforms, standards, and reporting processes to reduce duplication and promote interoperability across government.
- **Risk Technology Management**
 - Applies structured risk assessments to digital systems, data practices, and technology operations to support secure and reliable service delivery.
- **Oversight of Automated Decision Systems**
 - Imposes requirements for transparency, assessment, and monitoring of automated decision tools to ensure responsible and accountable use.
- **Performance Monitoring & Reporting**
 - Defines processes for tracking service performance, technology health, cybersecurity posture, and compliance with digital policy obligations.

What Does This Mean for Government?

The Directive on Service and Digital raises expectations for how federal departments manage digital services, technology operations, and data resources. Departments must show measurable improvement in service performance, cybersecurity resilience, and the coordinated use of enterprise tools. The Directive reinforces a more unified and accountable federal digital environment, where decisions about service design, technology investments, and data practices are guided by clear governance structures and government-wide priorities.

Key obligations include:

- **Adopting enterprise platforms** for identity, payments, cloud hosting, and digital credentials to improve and reduce system issues.
- **Enhancing cybersecurity readiness** by applying GC CSEMP, zero trust principles, and continuous risk assessments across digital systems.
- **Improving data governance** through consistent cataloging, metadata standards, retention schedules, and lifecycle management of information assets.
- **Ensuring services meet accessibility, bilingualism, and user-first standards**, embedding usability and inclusiveness throughout service design and delivery.
- **Establishing oversight for responsible AI and automated decision systems** to ensure transparency, human review, and compliance with federal AI requirements.

What Does This Mean for Industry?

The Directive on Service and Digital increases demand for technologies that help federal departments modernize digital services, improve cybersecurity, and strengthen data management. Vendors must show clear alignment with the Government of Canada standards and provide solutions that integrate smoothly with enterprise platforms and existing federal systems.

Procurement will prioritize offerings that demonstrate strong privacy, security, and responsible AI practices. This creates opportunities for providers of cloud services, cybersecurity tools, identity solutions, automation technologies, analytics platforms, and accessibility enhancements that support reliable, secure, and user-centric digital service delivery.

Key implications and opportunities for industry include:

- **Prioritization of solutions that align with GC enterprise standards:** including identity, cloud hosting, cybersecurity controls, digital credentialing, and interoperability requirements.
- **Growing demand for compliance ready offerings** that demonstrate strong privacy, security, and responsible AI governance, supported by clear documentation and auditability.
- **Opportunities for automation, workflow modernization, and digital service tools** that improve service performance, reduce manual burden, and support measurable outcomes.
- **Increased adoption of analytics and data enablement platforms** that strengthen metadata management, service monitoring, and decision support.
- **Continued need for accessibility, usability, and inclusive design solutions** that help departments meet statutory service and accessibility obligations.
- **Market opportunities for vendors specializing in modernization support services:** including cloud migration, system integration, cybersecurity readiness assessments, and data governance.

Provisions

Provisions	Description
Digital Governance Modernization	Requires departments to adopt enterprise solutions, governance boards, and integrated digital planning.
Cloud-First Architecture	Mandates prioritizing cloud services and API-driven platforms for modernized digital ecosystems.
Cybersecurity & Risk Management	Strengthens alignment to the GC Cyber Security Event Management Plan and zero trust principles.
Responsible AI	Requires adherence to AIA, transparency, auditability, and human oversight safeguards.
Data Stewardship	Establishes metadata standards, retention schedules, data quality controls, and privacy design requirements.
Service Delivery Standards	Mandates accessible, bilingual, user-centric services with performance monitoring and continuous improvement.

Contact Us:

Email: Research@carahsoft.com

See more from the Carahsoft Team:
To explore our catalog of federal, state, and local technology policies, executive orders, and directives shaping public sector modernization scan this QR code.

