Data your agency holds is public trust.

Can you prove to them it is governed, classified and traceable?

Using Collibra MCP to improve data classification and respond to Zero Trust requirements

Federal agencies and their international counterparts operate under heavy regulatory burden to protect citizens and their data. The requirements and trust are further tested with the capabilities of AI.

Data classification and organization are key to managing and protecting citizen data. Frequent needs include:

- The **Federal Risk and Authorization Management Program** (FedRAMP) governs cloud service authorization, with only about 19% of cloud providers needing Moderate baseline FedRAMP authorization having actually achieved it.
- The **Federal Information Security Modernization Act** (FISMA) requires agencies to continuously monitor, classify and secure all federal information systems.
- The **Freedom of Information Act** (FOIA) requires all agencies to respond to public records requests within 20 working days — a standard that federal agencies missed by an average of 240 days in 2025, when backlogs reached nearly 340,000 overdue requests, which is the highest ever recorded.

The problem is NOT one of policy. Every agency has policies.

The problem is data classification, evidence access and automation.

When an Office of Inspector General (OIG) auditor requests proof that an information system is properly classified and controlled, precision matters. When a FOIA request arrives for records spanning dozens of systems, delay shouldn't be a default. When a foreign oversight body requests transparency documentation under the United Kingdom's (UK's) Freedom of Information Act 2000, Australia's Freedom of Information Act 1982, or Canada's Access to Information Act, the evidence must be assembled manually, from systems that were never designed to support it.

 © 2026 Collibra. All rights reserved.

Collibra MCP connects third-party large language models (LLMs), including Claude, ChatGPT, Microsoft Copilot, and agents built on Databricks and Azure AI Foundry, directly to governed metadata, data lineage, classification records and business context in the Collibra Platform. Public sector data and compliance teams can ask questions in plain language and receive governed, audit-ready evidence assembled from the catalog automatically, without manual reconstruction under deadline pressure.

Where public sector agencies face the greatest regulatory evidence risk.

- **FedRAMP authorization evidence is labor-intensive to assemble and maintain:** As of early 2026, only about 19% of cloud providers requiring Moderate baseline FedRAMP authorization had actually achieved it. Federal GRC platforms that automate authorization evidence have reduced Authorization to Operate (ATO) timelines by 40 to 60%. Without governed data classification, lineage or access records, agencies cannot efficiently produce or maintain the evidence packages FedRAMP authorization requires
- **Supply chain and third-party data governance is a persistent gap:** The FISMA FY2023 report to Congress noted significant disparities in contractor and third-party security governance across agencies. Agencies cannot demonstrate FISMA compliance for systems operated or supported by third parties without governed lineage, access records and classification coverage that extends beyond the agency boundary
- **Controlled Unclassified Information (CUI) is ungoverned across agency systems:** National Archives and Records Administration (NARA) requirements and Executive Order 13556 require agencies to classify and control CUI consistently. Most agencies cannot systematically identify which systems hold CUI, apply consistent handling markings or produce evidence that CUI has been protected in compliance with applicable safeguards
- **International equivalents carry comparable exposure:** The UK Freedom of Information Act 2000 requires public authorities to respond to information requests within 20 working days, with enforcement by the Information Commissioner's Office (ICO). The Data (Use and Access) Act 2025, which received Royal Assent in June 2025, introduced new data governance obligations for UK public bodies. Australia's Freedom of Information Act 1982, Canada's Access to Information Act and the European Union's (EU's) Regulation 1049/2001 on public access to documents all impose parallel transparency and data governance obligations — each with their own classification requirements, redaction standards and response timelines that manual processes can't reliably meet
- **FISMA continuous monitoring requirements exceed manual capacity:** FISMA requires agencies to develop, document and implement agency-wide information security programs and report continuously on system status, control effectiveness and incident posture
- **FOIA backlogs are at record levels and growing:** Federal agencies accumulated a backlog of nearly 340,000 overdue FOIA requests as of September 2025. Requesters waited longer than 240 days on average, in contrast to a 20-working-day statutory deadline. Full-time FOIA staff at major agencies decreased 16% between fiscal years 2024 and 2025, while backlogs across those agencies increased 27%. Without governed data inventories, agencies cannot locate responsive records reliably, redact them consistently or process requests at the volume the public demands

 © 2026 Collibra. All rights reserved.

You can't classify and manage data for which there isn't full awareness.

You can't demonstrate FedRAMP compliance for systems you haven't classified and cataloged.

The gap between public sector governance policy and governance evidence is a data classification, inventory and lineage problem. Here are the symptoms:

- No authoritative, continuously maintained inventory of information systems, data assets, classification levels and ownership across the agency
- Controlled Unclassified Information not classified or tagged consistently across structured and unstructured data holdings
- FOIA-responsive records spread across email, document repositories, collaboration tools and legacy systems without governed metadata or search capability
- FedRAMP and FISMA evidence assembled manually for each authorization cycle rather than drawn from a continuously governed catalog
- International equivalents governed by separate, disconnected manual processes with no common data foundation
- Supply chain and third-party system data not covered by agency governance programs

Collibra MCP for Public Sector: Four regulatory workflows

With Collibra MCP, a data steward locates all agency information system assets and confirms classification, ownership and control status through the catalog. A data engineer traces data flows between systems to verify boundary definitions and identify unclassified or improperly governed assets. A Chief Information Security Officer (CISO) confirms that control results, access records and incident logs are linked to governed system assets and that the evidence package is current and audit-ready. Annual FISMA reporting is drawn from the catalog, not reconstructed from memory.

FedRAMP Authorization to Operate Evidence Package

FedRAMP authorization requires cloud service providers and agencies to demonstrate that data classification, access controls, lineage and security boundaries are documented, governed and auditable. Assembling and maintaining the evidence package manually is one of the primary reasons ATO timelines extend by months.

With Collibra MCP, a privacy analyst locates all data assets processed by a cloud service and confirms classification, sensitivity labels and data handling requirements through the catalog. A data engineer traces lineage from agency source systems through the cloud service environment to verify boundary definitions and data flow documentation. A catalog admin confirms that data contracts covering the cloud service include applicable security controls, audit trail provisions and freshness requirements. The FedRAMP evidence package is assembled from governed records, not from a documentation sprint.

 © 2026 Collibra. All rights reserved.

FOIA Request Fulfillment and Redaction Support

With Collibra MCP, a FOIA analyst instructs a connected LLM in plain language to locate all records relevant to a request across cataloged systems, email, document repositories and collaboration tools. The MCP server retrieves asset metadata, ownership records, classification tags and applicable exemptions from the catalog. The privacy officer confirms which records contain personally identifiable information (PII), CUI or other exempt categories, and generates a redaction guidance record linked to the specific request. The FOIA response package is assembled from governed records, with a defensible exemption log, rather than reconstructed from unstructured sources.

Controlled Unclassified Information Classification and Handling Audit

With Collibra MCP, a privacy analyst locates all agency data assets and applies CUI data class tags across structured databases, file shares, email and document repositories using the catalog's classification capabilities. A data steward confirms that handling markings, access controls and dissemination restrictions are documented for each CUI asset. A privacy officer generates an audit record demonstrating consistent CUI identification, marking and safeguarding across the agency data estate — satisfying NARA audit requirements and supporting FISMA control evidence simultaneously.

Key outcomes

Public sector governance evidence assembled from the catalog, not from manual reconstruction.

Collibra MCP transforms public sector regulatory compliance response across FISMA, FedRAMP, FOIA and international equivalents from a manual, deadline-driven process into a governed, repeatable, AI-assisted workflow. Systems are classified. Records are inventoried. CUI is tagged. FOIA-responsive assets are findable. When an OIG auditor arrives, a FOIA request lands, or a foreign oversight body requests documentation, the evidence is assembled from the catalog in hours, not weeks.

Collibra Public Sector

Purpose-built for the federal and global public sector data challenge. From system classification to CUI governance, FOIA fulfillment and FedRAMP authorization evidence, Collibra Public Sector and Collibra MCP unifies governance across every dataset, system and mission, so agencies can demonstrate accountability to the public they serve.

Learn more:
https://www.collibra.com/products/mcp-server

Collibra Public Sector © 2026 Collibra. All rights reserved. | publicsector.com

Sources

1. Qualysec, "FISMA vs. FedRAMP: Key Differences, Requirements, and Compliance Path," Aug. 2, 2026. As of early 2026, only about 19% of cloud providers needing Moderate baseline FedRAMP authorization had actually achieved it. https://qualysec.com/fisma-vs-fedramp/

2. Diligent, "From Spreadsheets to Real-Time: How Federal Agencies Are Modernizing FISMA, RMF and Zero Trust Compliance," Aug. 19, 2026. FedRAMP-authorized GRC platforms have helped agencies reduce ATO timelines by 40 to 60%. https://www.diligent.com/resources/blog/modernize-federal-agency

3. FOIA Advisor, citing New York Times analysis of FOIA.gov data, July 29, 2026. Federal agencies accumulated a backlog of nearly 340,000 overdue FOIA requests as of Sept. 30, 2025. Requesters waited longer than 240 days on average to hear back from federal agencies, against a 20-working-day statutory deadline. https://www.foiaadvisor.com/foia-blog/2026/7/29/foia-news-nyt-report-on-foia-requests-in-limbo-or-unfulfilled

4. U.S. Office of Government Information Services (OGIS), FOIA Ombudsman 2026 Annual Report for Fiscal Year 2025, Appendix B. Full-time FOIA staff at Cabinet-level departments and independent agencies decreased 16% between FY2024 and FY2025, while backlogs increased 27%. https://www.archives.gov/ogis/about-ogis/annual-reports/ogis-2026-annual-report-for-fy-2025-appendix-b

5. Open the Books, "40 Months? The Eternal FOIA Backlog," July 17, 2025. Complex FOIA requests had an average response time of 267 days across 416 agencies. Simple requests took an average of 39 days, but 31 agencies exceeded 100 days for simple requests on average. https://openthebooks.substack.com/p/40-months-the-eternal-foia-backlog

6. ExecutiveGov, "Latest FISMA Report Shows Increase in Cyber Incident Reports in FY 2023," citing OMB FISMA Annual Report to Congress. Federal agencies reported 32,211 cybersecurity incidents to CISA in FY2023, a nearly 10% increase over the prior year. https://www.executivegov.com/?p=259936

7. OMB Memorandum M-25-04, "Fiscal Year 2025 Guidance on Federal Information Security and Privacy Management Requirements," Jan. 15, 2025. FedRAMP Marketplace data automated into FISMA reporting; agencies directed to prepare for machine-readable performance and incident data submissions. https://bidenwhitehouse.archives.gov/wp-content/uploads/2025/01/M-25-04-Fiscal-Year-2025-Guidance-on-Federal-Information-Security-and-Privacy-Management-Requirements.pdf

8. ICO and UK Parliament. Data (Use and Access) Act 2025 received Royal Assent on June 19, 2025, amending the UK General Data Protection Regulation (GDPR) and introducing new data governance obligations for UK public bodies. https://www.clym.io/regulations/uk-general-data-protection-regulation-uk-gdpr

9. Collibra Product Innovations. Collibra MCP server generally available November 2025. Enables AI/ML developers, business users, and LLMs to access and engage with governed metadata and business context in the Collibra platform. https://www.collibra.com/products/innovations

10. Collibra Marketplace, "Databricks MCP Marketplace: Collibra MCP Server." The MCP server addresses inconsistent context retrieval, fragmented integration workflows, and lack of standardized communication between Collibra and other information sources. https://marketplace.collibra.com/listings/databricks-mcp-marketplace-collibra-mcp-server/

 © 2026 Collibra. All rights reserved.