



**Issue Paper on Federal Information Technology Management
2026 Bipartisan Government Reform Roundtables
U. S. Senate Homeland Security and Governmental Affairs Committee
June 24, 2026**

This paper was prepared by members of the Shared Services Leadership Coalition (SSLC) Board of Directors and Advisory Board.

I. ISSUES AND CHALLENGES

1. Fragmented and Outdated Congressional Approach to IT Management and Budgeting

Congress lacks a unified, outcomes-driven framework for Federal agency guidance on IT modernization. Measurable goals are rarely stated by authorization, oversight, and appropriations committees for key IT spending metrics such as improvement in mission outcomes, reduction in unit costs, cost savings, or percentage allocations for legacy O&M and modernization. This fragmentation prevents consistent oversight, inhibits cross-committee alignment, and leaves agencies without clear understanding of legislative expectations for modernization outcomes, return on investment, or performance improvement.

The statutory framework governing Federal IT is similarly outdated. Foundational laws in Titles 5, 40, 41, and 44—including the Privacy Act, Paperwork Reduction Act, FITARA, FISMA, the E-Government Act, Evidence-based Policymaking Act, and the Clinger-Cohen Act—no longer reflect the realities of modern technology, consumption and operational models, or data governance and practices. Roles and authorities for CIOs, CTOs, and CDOs (among others) remain inconsistent across statutes, creating ambiguity and compliance burdens that rarely improve mission outcomes. Lacking clear expectations on specific goals or Congressional prerogatives, current laws have become burdensome compliance exercises with little impact on results.

Additionally, the appropriations structure reinforces siloed IT management. Funding tied to decades-old program structures prevents enterprise modernization and constrains customer-centric service delivery. Siloed funding also impedes enterprise IT management and optimization, contributing to duplicative systems, inconsistent data, and higher long-term costs.

2. Ineffective Executive Branch Management of Technology, Data, and Modernization

Agencies face persistent gaps in the skills needed to manage large-scale modernization projects. Enterprise architecture, alternatives analysis, program management, benchmarking, and change management expertise remains scarce. Program executives often have limited visibility into how



technology can transform operations, while CIOs may lack sufficient mission knowledge and business credibility to effectively partner with program leaders on modernization initiatives.

Cultural and legal barriers further impede transformation. Protective agency cultures resist change and prioritize autonomy, and trust between program executives and CIOs is often weak. Conflicting authorities among CIOs, CDOs, CAOs, CISOs, and program leaders create fragmented accountability for modernization and data management. Opportunities to deliver more integrated, customer-centered services are limited by agencies' lack of trust in data and systems operated by different program teams within and across agencies. This reluctance to share and use information across organizational boundaries prevents governments from simplifying customer interactions, reducing errors, consolidating redundant systems, and improving service outcomes.

Dependence on legacy systems remains a major obstacle. Chronic underinvestment in modernization has produced a landscape of at-risk platforms and disproportionate spending on labor-based O&M contracts tied to highly customized legacy systems. This crowds out modernization funding and prevents agencies from adopting IT-as-a-Service models that could reduce costs, fix chronic data problems, and improve performance – and these issues must be addressed before agencies can contemplate the widescale use of artificial intelligence in mission areas.

Data fragmentation compounds these challenges. Agencies generally have immature data governance (e.g., data standards and stewardship structures), and the Evidence Act data governance reforms have not worked as intended. The existence of multiple “authoritative” databases for programs serving similar missions results in inconsistent and conflicting data in systems of record and often drives agencies to add systems that aggregate data rather than fix the underlying redundancy and data governance issues.

The Federal Government’s current practice can be described as “collect many, use many.” This approach creates unreliable data for anti-fraud purposes and exacerbates data collection burdens in “collect many, use once” information sharing. For example, the use of “collect many, use once” in verifying citizenship failed to provide appropriate privacy protections and limit erroneous decisions, as highlighted in *League of Women Voters et.al. vs. Department of Homeland Security* (Civil Action No. 25 - 3501).

These Federal practices contrast starkly with common industry approaches (e.g., Amazon) that feature a single, authoritative data model for access by all customers to simplify transactions for



all users. Similarly, the government of Australia’s lifelong citizen ID is enabled by “collect once, use many” data practices.

3. Ineffective Contracting for IT Modernization

Federal budgeting and procurement practices are misaligned with modern technology markets. Agencies continue to buy labor rather than outcomes, while the IT industry has shifted to consumption-based, subscription, and performance-based models. This creates a Federal IT supply chain that is increasingly separated from IT trends and modernization.

Legacy systems are difficult to retire due to inaccessible data formats and long-term data retention requirements. Agencies often keep legacy systems solely to access legacy data, perpetuating parallel operations and inflating O&M costs.

4. Ineffective Approaches to AI Adoption

AI adoption in the Federal Government is following the same pattern as early SaaS and website proliferation—rapid, ungoverned, and fragmented. Agencies pursue isolated use cases without enterprise strategy, risk management, or measurable ROI.

Moreover, weak data foundations limit AI’s value. Fragmented architectures and outdated data structures prevent agencies from deploying AI at scale or achieving meaningful mission outcomes. As AI costs shift toward consumption-based models, the lack of enterprise governance risks dramatic increases in agency IT budgets that will quickly crowd out necessary investments for mission programs.

II. OPTIONS

1. Rationalize Government-Wide IT Governance

Congress and OMB can strengthen modernization by clarifying authorities, aligning goals, and increasing accountability, especially by revisiting the underlying legislative framework that has proven so ineffective in today – and tomorrow’s – technology ecosystem. Congress would be wise to prioritize these efforts before adding more siloed, targeted legislative activity that would likely compound this problem. As a starting point, HSGAC should require agency Deputy Secretaries to testify regularly on poor-performing IT projects, data governance and quality, codifying IT Dashboard transparency, and shifting IT oversight from cost-center management to mission-outcome investment. Strengthening collaboration across oversight, authorization, and appropriations committees would improve alignment of IT spending with modernization goals.



2. Modernize Capital Budgeting and Acquisition

Congress can modernize capital budgeting by reinforcing business case requirements, mandating analysis of alternatives for major legacy systems, and establishing minimum ROI thresholds tied to cost reduction or mission improvement. Congress should require OMB to assess whether agencies could use a shared services solution before approving a siloed acquisition for all modernization initiatives. Agencies should be required to share business cases above a defined threshold with Congress and include modernization ROI data in Congressional Budget Justifications.

Working capital fund authorities and multi-year funding mechanisms should be updated to accelerate modernization. Congress can also set clearer expectations for O&M versus modernization spending ratios and require agencies to report progress against outcome-based modernization targets.

3. Reform Contracting and Procurement

Contracting reforms should shift agencies from labor-based O&M contracts to performance-based models, including updated transparency requirements under the Service Contract Inventory Act. OMB should be held accountable for ensuring agency contracting aligns with modernization priorities and outcome-based performance goals.

4. Strengthen Performance Management and Oversight

Congress can require agencies to adopt rigorous performance measures, cost and schedule targets, and analysis-of-alternatives processes. Deviations of 20 percent or more should trigger reporting to Congress. Agencies should also be required to reduce legacy spending over time, quantify the opportunity costs of maintaining legacy systems, and accelerate modernization through shared services and IT-as-a-Service models. OMB and Treasury should fix the USASpending and Performance.gov data governance, including data quality and timeliness, related to IT projects and procurement to give Congress visibility into major IT investments and enable more consistent oversight. This will become more critical in the future as agencies invest in agentic AI for modernization and transformation.

III. HARD QUESTIONS

1. Can Congress produce a comprehensive legislative modernization package, or must reforms be sequenced—and if so, in what order?



2. How can Congress drive agency executives to accelerate the shift from legacy O&M to modernization, and from labor-based to performance-based contracting?
3. How should Congress define success for more than \$100B in annual IT spending – ROI, productivity gains, or targeted shifts in modernization versus legacy spending? Should the metrics for ROI for AI be different than other modernization efforts?
4. Does the Federal government have enough skilled program managers and risk-management experts to oversee government-wide modernization?
5. How can cultural resistance -- including concerns from employees and unions about job impacts, and whether the role of the Chief Data Officer envisioned in the Evidence Act is sufficient to address government data problems -- be addressed to enable transformation?
6. How will large-scale modernization and agentic AI reshape the composition and skill requirements of the Federal workforce?

IV. RECOMMENDED PARTICIPANTS

SSLC has nominated the following experts to speak to these challenges (not in preferred order):

Matthew Cornelius, SSLC Board of Directors and Managing Director, Industry Strategy, Workday
Mark Forman, SSLC Advisory Board and former Federal CIO