

March 2025

American P.I.E.

How **Productivity**,  
**Innovation**, and  
**Efficiency** Can  
Transform American  
Government

TECHNOLOGY CEO  

---

COUNCIL

**Cristiano R. Amon**  
President and CEO  
Qualcomm Incorporated

**Safra Catz**  
CEO  
Oracle Corporation

**Michael S. Dell**  
Chairman and CEO  
Dell Technologies

**Arvind Krishna**  
CEO  
IBM Corporation

**Enrique Lores**  
President and CEO  
HP Incorporated

**David Zinsner**  
Interim CO-CEO & CFO  
Intel Corporation

# About The Council

The Technology CEO Council (TCC) is the information technology industry's leading public policy advocacy organization comprised exclusively of chief executive officers from America's top information technology companies.

For 37 years, the Technology CEO Council, formerly known as the Computer Systems Policy Project, has focused on advancing policies that promote innovation and U.S. competitiveness through technology leadership. Our CEOs engage policy makers on issues of importance to the nation, offering insights and recommendations on ways technology can help solve critical challenges.

Currently, the TCC is driving public policy initiatives related to American leadership in emerging technologies (including artificial intelligence, quantum, and next-gen semiconductors); ensuring a competitive business climate for U.S. innovators (focused on tax, trade, and regulatory policies); and leveraging technology to advance the national interest (via government efficiency, defense modernization, and economic productivity).

The Technology CEO Council includes some of the world's best-known technology brands and leaders, generating more than \$350 billion in annual revenues and employing more than 700,000 workers.

# Contents

- ABOUT THE COUNCIL** ..... 1
- EXECUTIVE SUMMARY** ..... 3
- INTRODUCTION** ..... 6
- COST EFFICIENCY OPPORTUNITIES** ..... 9
  - Productivity ..... 10
    - Public-Private Partnerships For Shared Services ..... 10
    - Fraud And Improper Payments Prevention ..... 13
  - Innovation ..... 17
    - Artificial Intelligence (AI) ..... 17
  - Efficiency ..... 19
    - IT Modernization and Cloud Adoption ..... 19
    - Cybersecurity ..... 22
    - IT Financial Operations (FinOps) ..... 24
- APPENDIX: SCORING ADMINISTRATIVE SAVINGS** ..... 25
- CONCLUSION** ..... 28
- REFERENCES** ..... 29



# EXECUTIVE SUMMARY

For the past several decades, government leaders concerned about rising U.S. deficits have had only two options: higher taxes (slowing the economy) or big spending cuts (potentially undermining critical missions). Doing nothing meant ever-greater national debt, which is today higher as a share of the U.S. economy than at any point in the past 150 years.

There is a third option. IT modernization, business process innovations, and artificial intelligence (AI) capabilities collectively present a new pathway out of this Hobson's choice. By adopting these approaches, **the U.S. government can reduce operational costs and increase productivity for the taxpayer by \$2 trillion over 10 years, while simultaneously improving service quality and impact.**

Although government operations have unique demands that prevent consistently achieving private-sector efficiency levels, significant improvements are possible. By implementing modern, interconnected processes and systems, government agencies can meet their missions more quickly, at a lower cost, and with reduced risk. Technologies available today enable faster decision making, better coordination among agencies, improved security, and more responsive services for citizens.

This report identifies several key areas for improving cost effectiveness over the next decade, including through fraud and improper payments prevention, artificial intelligence, IT modernization, shared services, financial operations (FinOps), and legacy application modernization.

To achieve major cost efficiencies, this report recommends the CIOs and other agency leaders incorporate industry best practices and prioritize and sequence implementation efforts. These steps can ensure that the cost reduction opportunities identified are successfully achieved, leading to a more efficient and effective federal government that better serves the public.

By adopting modern technologies and implementing the recommendations in this report, the President can establish a foundation for substantial improvements in cost effectiveness over the next decade. The potential benefits are significant—not only in terms of efficiency, but also in enhancing the overall effectiveness of government operations, ultimately benefiting the American public. It's time to act boldly.

Cost efficiency estimates, highlighted in the table below, were derived through analysis of specific examples featured throughout this report. These estimates are based on real experiences in both public and private sectors, extrapolated to reflect the size and scope of the federal government based on data from the Office of Management and Budget (OMB) as of January 2025. Assuming effective implementation and sufficient resource capacity to carry out these recommendations, cost efficiency figures reflect the total estimated opportunity over a 10-year period, and may necessitate additional investments in people, process and technology. Further analysis would be needed to determine what percentage of the efficiencies identified in this report represent cost reduction opportunities that are "scoreable" by Congressional Budget Office (CBO) standards (see Appendix). A more refined estimate of scoreable savings would require further review with OMB and CBO.

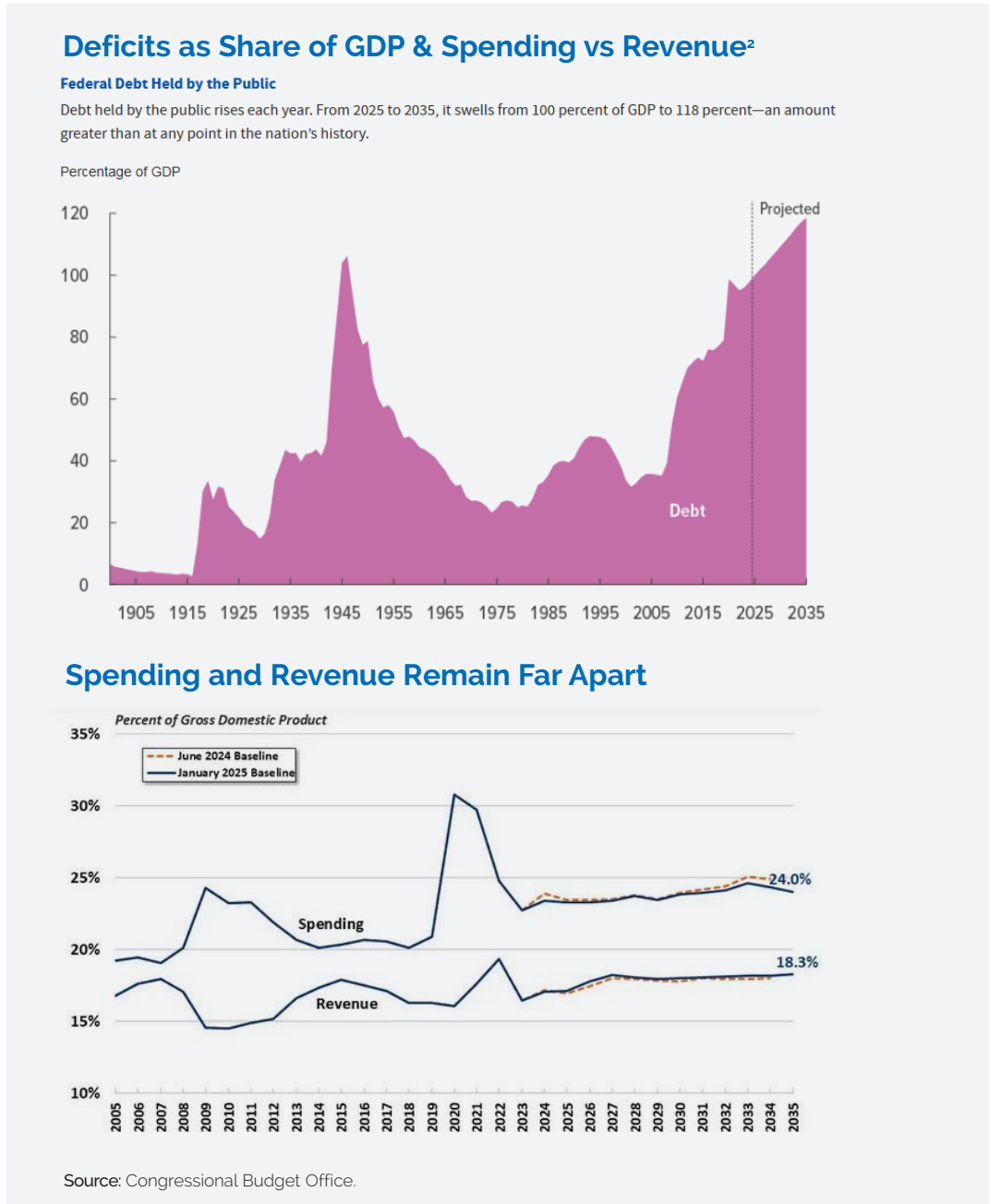
10-YEAR COST EFFICIENCY OPPORTUNITIES <sup>1</sup>	
COST EFFECIENCY AREA	ESTIMATED 10-YEAR COST AVOIDANCE
Shared Services	\$75 Billion
Improper Payments Prevention	\$760 Billion
Artificial Intelligence	\$345 Billion
IT Modernization and Cloud Adoption	\$170 Billion
Cybersecurity	\$500 Billion
FinOps	\$150 Billion
<b>TOTAL 10-YEAR COST IMPACT POTENTIAL</b>	<b>\$2 TRILLION</b>

1. A review of these opportunities should assess the degree to which any figures already have been incorporated into the CBO baseline. A portion of the cost reductions included in this table and further described throughout this report may be underway already through current investments and initiatives or may be subject to overlap across initiatives, which could reduce new savings opportunities in some areas. In addition, any review of opportunities should include a detailed estimation of any additional investments required to achieve these savings.



# INTRODUCTION

The United States operated at a \$1.83 trillion budget deficit in Fiscal Year (FY) 2024. The United States has only experienced a fiscal year-end budget surplus four times in the last 50 years, most recently in 2001. National debt as a share of GDP will soon exceed the previous highs caused by World War II, with spending consistently outpacing revenues.



2. From <https://www.crfb.org/blogs/cbo-releases-january-2025-budget-and-economic-outlook> and <https://www.cbo.gov/publication/61172>.

The Trump administration thus inherits a challenging fiscal position, which has grown in magnitude for more than two decades. The administration and Congress have a critical opportunity to rethink how to reduce costs across the government, while maintaining or improving the quality of services for the American public.

Leveraging AI technology, business process innovations, cloud native applications, and strategic partnership solutions, government can operate smarter, more cost effectively, and with greater security. The implementation of modern, interconnected technologies, and business processes presents an opportunity to realize sustainable cost reductions and avoidance of \$2 trillion in the next 10 years.

Prior studies have suggested cost savings opportunities approaching this estimate. The Government Accountability Office issued a 2022 report that identified savings opportunities in the tens of billions of dollars range from 94 separate actions.<sup>3</sup> More recently, McKinsey & Company issued a report estimating federal savings opportunities of \$285-295 billion annually from productivity improvements, and \$725-\$765 billion adding in state and local government.<sup>4</sup>

Achieving this level of savings and efficiency will necessitate technology adoption to promote effective government operations.<sup>5</sup> For example, in 2019 U.S. Chief Information Officer (CIO) Suzette Kent cited significant savings from robotics process automation.<sup>6</sup> Expanding current efforts to modernize the federal IT portfolio and the processes that support it will add value by enabling agencies to meet their missions more quickly and completely, with less overhead, at lower cost and with reduced risk.

This report highlights the necessity for innovation to modernize government IT, and the focus throughout the report is to enable the transformation of the American government with a focus on:

- Productivity
- Innovation
- Efficiency

The recommendations in this report can support the Trump administration by adapting commercial practices to help agencies achieve the benefits of modernization.

---

3. <https://www.gao.gov/products/gao-22-105301>.

4. <https://www.mckinsey.com/industries/public-sector/our-insights/us-government-productivity-a-more-than-2000-per-resident-opportunity>.

5. The cost reduction rates realized in the examples in this report are based on real experience in the public and private sectors, and have been extrapolated to reflect the scope of the federal government. As such, they should be viewed as estimates for potential achievements based on effective implementation at a governmentwide scale, and not precise budget forecasts.

6. <https://fedscoop.com/rpa-savings-federal-agencies-reinvest-suzette-kent/>.



# COST EFFICIENCY OPPORTUNITIES

# Productivity

## Public-Private Partnerships for Shared Services

The government can eliminate waste and streamline back-office operations through expanded use of commercial shared services platforms.

The issue of government waste is a longstanding concern recognized by government oversight efforts for decades. Federal agencies spend billions of dollars each year on programs and activities that are duplicative or overlap with other programs, which diverts resources away from other critical priorities and undermines the efficiency and effectiveness of those operations. Legacy IT systems, cumbersome administrative processes and regulatory requirements, and limited resources impede the functioning of government agencies, significantly impacting the productivity of federal employees and the overall efficiency of agencies.

The impact of government waste in back-office operations, such as human resources and payroll, is significant and far-reaching. These functions consume a substantial portion of the federal budget, often at the expense of mission-critical priorities like national defense and border security. By empowering shared service providers, potential cost savings are significant. For governmentwide back-office operations, cost efficiencies from shared services implementation over 10 years is estimated to be as much as \$75 billion.<sup>7</sup>

There are currently five federal and one private shared services center (SSC) operating to support the government in the areas of human resources and payroll today, representing the highest rate of adoption across government. These SSCs have proven how the shared services operating model can drive efficiency and save money.



7. [SSLC-Proposal-for-Transforming-Government-Operations-12-17-24.pdf](#).

Realizing these benefits requires bold action. To accelerate the achievement of results, the government needs a paradigm shift—moving away from spending resources on federalizing untested solutions and instead, accelerating the transition to proven, operational commercial cloud-based platforms.

The government wastes hundreds of millions of dollars due to outdated and ineffective solutions. Many customers of federal providers express dissatisfaction with the services they receive, leading them to invest hundreds of millions in developing and maintaining their own systems to fill the gaps left by existing solutions. By driving higher adoption of more modern shared services, agencies can reduce operating expenses and eliminate the duplicative investment, doubling the impact of efficient government operations. Specific actions to achieve this goal follow.

**Learn from past failures.** Large-scale modernization efforts for existing platforms have proven to be expensive and ineffective. For instance, a 10-year, \$2.5 billion blanket purchase agreement awarded by one agency in 2018 to modernize federal payroll was unsuccessful in completing the proof-of-concept phase. Similarly, a \$75-million contract awarded by an agency in the same year to modernize their human resources solution failed to deploy after six years, with an additional \$250 million contract planned. These and other examples underscore the significance of avoiding costly modernization efforts that may not yield the expected outcomes. Agencies should avoid the “if you build it, they will come” fallacy; costly modernization efforts do not always yield expected results and can be more expensive in the long-term.

**Focus on proven solutions.** Rather than investing in lengthy modernization projects that are high-risk efforts to re-invent existing solutions and bring a low likelihood of on-time, on-budget implementation, the federal government should concentrate on expanding platforms that have already demonstrated effectiveness. For example, IBM has a history of successfully delivering human resource (HR) and payroll services to the federal government for over a decade. By focusing on existing, competitive commercial providers, agencies can capitalize on the expertise and investments in innovation to maximize the advantages of shared services.

As a use case, in 2024, the Marine Corps became the first and only military service to successfully complete a financial audit of its assets and inventories. In 2025, it again achieved a clean and successful audit and was the only service to do so. The agency did so by migrating to a general ledger system supported within the Defense Agency Initiative (DAI), which was interoperable with the Corps' financial, personnel, and logistics systems. DAI was already widely in use at the Department of Defense (DoD). By choosing to embrace an established and successful system, rather than purchasing a new one, the Marine Corps became the first and only military service to reach the clean audit milestone. DAI's core functionality is based on commercially available enterprise resource planning (ERP), financial, and logistical applications from Oracle. By leveraging commercial technologies, the Corps and 27 DoD agencies have adopted auditable, CFO Act-compliant technologies, which have enabled them to deliver reliable, useful, and timely financial information to support DoD's financial management goals.

Advantages federal agencies can receive by adopting more modernized shared services platforms include:

**Enhance Mission Focus:** Agencies become more productive, avoiding focus on back-office operations and concentrating on activities that advance the agency's core mission. Specifically, federal agencies should utilize solutions that drive efficient mission outcomes at the edge. For example, HP has worked with military agencies to optimize end-user hardware while deploying hundreds of thousands of devices globally, improve resource utilization and increase asset utilization via Lifecycle Services, advance endpoint security via firmware resiliency, and reduce licensing costs and power consumption. At the same time, such solutions have been utilized by civilian agencies to improve the efficient delivery of services and streamline secure supply chain practices.

**Reduce Costs:** Standardized and automated transactional processes simplify complexity, eliminate processing errors, and reduce technical infrastructure costs. While the public sector has seen some success with HR and payroll shared services, many federal agencies have yet to replicate the benefits enjoyed by their commercial counterparts. Leveraging commercial capabilities for HR and payroll shared services offers federal agencies access to the most efficient transition service, modern solutions, and predictably low operations and maintenance (O&M) costs that are not available with current public providers. For example, analysis has shown that the Social Security Administration (SSA) can reduce overall HR spend by 25 percent in 18 months by leveraging a federally proven cloud based commercial HR shared services solution.

**Deliver Efficiencies through AI:** Digitizing and automating administrative tasks and enabling data-driven employee self-service capabilities can help boost productivity and reduce administrative burdens, enabling human resources professionals to do more with less. Many federal agencies miss out on enabling a cross-agency, industry-hosted shared service platform with tools such as AI-enabled assistants for employee self-service, and on automated human resources tasks such as payroll, benefits administration, time entry, and performance management.

**Provide greater value through commercial models:** Industry-based, proven assets are operating in the federal space today and are ready to scale. Agencies can leverage public-private partnerships to continually modernize services. For example, IBM provides commercial shared services in the federal government today, currently serving over 500,000 federal employees. IBM's Federal HR Cloud is a cloud-based, software-as-a-service solution that offers the configurability and flexibility required to accommodate complex and dynamic federal HR and payroll requirements. The IBM solution delivers modernized functionality for the complete suite of HR and payroll processing, including employee and manager self-service, time and labor, benefits administration, performance management, talent acquisition, and talent development.<sup>8</sup>

---

8. [https://newsroom.ibm.com/2023-08-30-IBM-Receives-FedRAMP-Authorization-for-its-Federal-HR-Shared-Services-Solution?mhsrc=ibmsearch\\_a&mhq=Federal%20Shared%20Services](https://newsroom.ibm.com/2023-08-30-IBM-Receives-FedRAMP-Authorization-for-its-Federal-HR-Shared-Services-Solution?mhsrc=ibmsearch_a&mhq=Federal%20Shared%20Services).

## Fraud and Improper Payments Prevention

The federal government must address the persistent challenge from fraud, waste, and abuse due to inefficient processes, inadequate oversight, and vulnerabilities in financial systems in order to better allocate taxpayer funds and strengthen public trust.

Improper payments, including fraud, are long-standing and significant problems in the federal government. The U.S. Government Accountability Office (GAO) reported<sup>9</sup> in September 2024 that since fiscal year 2003, cumulative “reported” improper payment estimates by executive branch agencies have totaled around \$2.7 trillion, the actual number being likely higher when considering unreported fraud that can only be estimated. Like an iceberg, there is much more unseen compared to what is seen—two-thirds of the actual leakage may not be known. In April 2024, GAO estimated total direct annual financial losses across the government from fraud alone to be between \$233 billion and \$521 billion, based on data from fiscal year 2018 through fiscal year 2022.<sup>10</sup>

Fraud involves an *intentional* act of deception for the purpose of producing an undue financial gain. While other types of improper payments, (including waste, abuse, and error) can be addressed through remediation and training, fraud can only be remediated by stopping fraudulent payments and punishing the criminals perpetuating them.

The behavioral aspects of fraud make it difficult to quantify because the perpetrators take extraordinary steps to make their payments look proper. Other forms of improper payments can be easier to detect and measure as they are not obfuscated, and agencies can compare what happened to what was expected to happen. Reducing all forms of improper payments, including fraud, is a key pathway to improve solvency—without reducing benefits or seeking additional funding. Based on analysis of opportunities identified by GAO and other studies, effective implementation of payment integrity reforms could help agencies reduce improper payments by \$760 billion over 10 years.



9. <https://www.gao.gov/products/gao-24-107660>.

10. <https://www.gao.gov/products/gao-24-107660>.

## Findings for Reducing Improper Payments

The April 2024 GAO Report recommended actions that agencies could take to reduce improper payments. These include improvements in reporting, use of analytics, internal controls, data sharing, and clarifying responsibility for improper payments within each organization.

Building on these recommendations and in light of practices proven effective in industry, government agencies should focus on actions in nine specific areas to reduce improper payments. A recent report<sup>11</sup> from the IBM Center for The Business of Government laid out a framework for agencies to follow that is based on commercial best practices, including nine specific actions that agencies can take to drive efficiencies in this area.

Given the sheer number of transactions the government makes across more than \$6 trillion in annual spending, it is imperative that technology lead the way in establishing payment integrity in the federal government. The government can adopt multiple actions to achieve this goal.

## Use AI to Reduce Improper Payments

Across these key focus areas, AI will play a pivotal role in reducing improper payments—especially when adversaries use their own artificial intelligence against the government to take over accounts and spoof authority.

In general, AI can drive two important outcomes:

1. **Improved Analytics.** The use of AI algorithms to detect anomalous behaviors—by analyzing vast datasets to spot anomalies, identify patterns, and alert on changes that may indicate improper activity—will be key to reducing the impact of fraud, waste, abuse, errors, and all forms of improper payments
2. **Improved Automation.** The use of generative AI to automate processes that cannot be completed in time or at scale by humans alone, especially those that require reading large or complex documents to ensure payment integrity, will be required. Generative AI can ensure that payments are fast and proper.

Machine learning and more sophisticated unsupervised models can be used to identify and predict risk patterns in transactional and historical data. At the same time, AI-enhanced biometric and behavioral authentication methods can prevent and recognize identity theft and unauthorized access systems and accounts.

Generative AI can help automate labor-intensive tasks such as reviewing documents, curating data to ensure a payment is proper per standing policy documents. For example, AI-driven solutions can ensure proper payments in the area of medical claim processing. AI can perform a check to confirm payment integrity before making the payment. By using digital assistants to read and summarize pre-authorization reports and compare with medical records, agencies can ensure that the treatment provided matches the treatment authorized and then confirm that the services billed all match.

---

11. <https://www.businessofgovernment.org/report/enhancing-government-payment-integrity-leveraging-ai-and-other-emerging-technologies>.



Historically, it was not possible to perform such a review and meet rapid payment obligations; payments were made that could not be confirmed as being proper. AI can also be used ensure that the amount billed is also proper. In a final step, AI can be used to help agencies decide on whether or not to release the payment, or if they should generate an alert for follow-up by an analyst. These steps have driven significant efficiencies in the financial services and health care sectors, and government can adapt and expand their application to achieve significant efficiencies in cost and delivery.

### Consider Scale

Fraudsters will always find the lowest barrier to entry. Often this will be to attack smaller programs that do not have the same resources and sophistication in stopping fraud and other forms of improper payments.

The Trump administration should consider creating a "Payment Integrity as a Service" capability, built around the nine points of focus above, that can be accessed by agencies and programs not large enough to justify their own internal investments in skills and technology.

For example, the Centers for Medicare & Medicaid Services (CMS) have a fraud detection unit to help identify and stop fraudulent healthcare claims. However, other large agencies processing similar claims do not have equivalent fraud detection capacities. Agencies could work together to share fraud detection services and investments, resulting in greater economies of scale, reduction of duplicative investments, development of best practices and, ultimately, lower costs and improved performance. By partnering with industry, this would also leverage commercial profit incentives to focus on stopping improper payments.

### Pursue Return on Investment

An effective payment integrity program prevents improper payments before they are made. That said, it is very difficult to measure the ROI on events that do not happen, constraining attempts to measure and encourage such efforts.

Agencies could reduce costs and improve solvency to produce multiple outcomes:

1. Returning 1-3 percent of a program's outflows. This is based on the expectation that 5-7 percent of a program's outflows are "improper." Recovering 25-50 percent of these losses would result in a conservative estimate of \$10-\$12 billion per year in reduced leakage.
2. Reducing the cost of compliance by 20-30 percent through digital assistants that can help agencies to ensure proper payments. Baseline on what "should be" spent, versus what is actually spent, the ROI could be much higher.
3. Reducing the cost of fraud operations by 20 percent while providing uplifted recovery. This would be related to investigations and discovery operations.

IBM is on the forefront of applying sophisticated AI-based automation to ensure payment integrity. IBM supports the Department of Veterans Affairs in using advanced AI to automatically read documentation sent by veterans to apply for benefits. The details are assessed to confirm the request is proper before it is submitted to fulfillment. This has reduced the value of improper payments while also reducing operational costs and improving the experience of the veteran. The majority of legitimate requests can be accelerated for immediate payment. In another example, IBM has worked with the IRS to leverage AI in identifying over \$17 billion in improper payments.

Additionally, working with Triwest, IBM provides real time fraud protection in line with claim payment processing for the Defense Health Agency (DHA). This first of a kind deployment applies real time fraud detection capabilities to the current claim payment processing capabilities. In the future, DHA expects to further automate the review of medical records, and match to both the claim and to the pre-authorization, to automate assessment of payment authenticity.

Today's most successful companies are moving from siloed to connected planning—and seeing better business performance as a result. The government needs to do the same. By providing a unified view of financial, operational, and line of business planning, embracing modern cloud applications improves planning accuracy and will make the government more agile while increasing transparency into government spending. Advanced technologies, such as AI, machine learning, and predictive analytics, enable finance teams to integrate real-time data into planning, eliminating delays in decision making. By moving to more modern commercial cloud-based applications, government can adopt data-driven predictions, AI-driven insight, and augmented intelligence.

# Innovation

## Artificial Intelligence

Artificial Intelligence can help agencies to make better decisions by automating manual tasks like data entry and form processing and analysis. AI can assist with streamlining workflows and providing real-time insights, democratizing skills, and enabling faster, more informed decision making. The Trump administration can adopt AI-powered automation tools across key agencies, while ensuring integration with existing systems for seamless adoption.

AI systems can perform tasks that have traditionally required human intelligence, such as learning and activities that require cognitive ability. AI can help agencies identify patterns and relationships and respond to queries that arise in complex scenarios.<sup>12</sup> AI technologies can also increase developer productivity, supporting modernization of old systems and bridging the skills gap between government and industry.

Building on recommendations made elsewhere in this report, the recipe for a more efficient U.S. federal government includes eliminating complexity, simplifying how work gets done, and automating manual tasks with AI—at scale. Analysis of industry best practice suggests that the federal government could save, on average, 10 percent on its operations and maintenance costs by implementing AI technologies, and could achieve a total of \$345 billion in cost efficiencies over 10 years.

There are abundant opportunities for AI-driven transformation of critical federal government programs to enhance efficiency, strengthen citizens' trust in government, and bolster security. For example, IBM's use of generative AI to modernize the IRS's 1960s-era code has significantly reduced processing time and improved code quality.

The beginning of a new administration provides a unique opportunity to ask fundamental questions about existing government programs and investments and how federal agencies can optimize the use of limited resources with AI solutions.

Federal agencies handle vast amounts of data and serve millions of people, from safeguarding identities and national security to managing benefits and citizens services. The concept of analytics and its applications have continued to evolve, and AI has driven efficiencies that will positively impact how the federal government operates now and in the future. AI can also augment and improve decision making across the federal workforce, freeing up time and energy for dedicated federal workers by automating data analysis, reducing manual tasks, integrating cross agency services, and minimizing errors in claims processing and system maintenance. While AI is not a cure-all, AI can have a transformative impact for government in the following key areas, consistent with objectives identified elsewhere in this paper:

---

12. [https://www.cbo.gov/publication/61147#\\_idTextAnchor000](https://www.cbo.gov/publication/61147#_idTextAnchor000).



- Accelerating speed and accuracy of decisions
- Unlocking human resources productivity
- Transforming how government modernizes IT
- Combating cyber-based threats
- Reducing fraud, waste, and abuse
- Accelerating claims processing

Through its use by the federal government, AI could affect both revenues and spending by increasing the efficiency of the government in collecting tax revenues and in distributing those revenues through transfer payments. AI also could enable improvements in the goods and services provided by the government, spurring federal programs to spend more to take advantage of the technology.<sup>13</sup>

To demonstrate an example of using AI to improve performance, the U.S. Air Force (USAF) struggled with managing and analyzing the vast data generated by advanced aircraft like the F-35, leading to delays in decision making and inefficient T&E methods. Dell developed the Quick Reaction Instrumentation Package (QRIP), a compact device that stores up to 1.2 terabytes of data, enabling rapid data access and analysis. The CHEETAS framework leveraged cloud and edge computing to streamline data processing and sharing. The solution significantly reduced post-mission debrief times, automated data mining and analysis with AI, and provided real-time insights, enhancing overall decision making for the USAF.

Additionally, IBM is working with Treasury in harnessing AI to combat taxpayer fraud, successfully recovering \$4 billion in fraudulent and improper payments. This success is primarily due to advanced machine learning (ML) techniques that analyze data to identify tax noncompliance.<sup>14</sup>

At SSA, integrating AI and automation throughout the end-to-end disability claims process will enable the agency to transform the program and deliver benefits to constituents faster and cheaper—improving end-to-end claims processing times by 95 percent.

---

13. <https://www.cbo.gov/publication/61147>.

14. <https://www.kiplinger.com/taxes/treasury-ai-catching-tax-cheats-and-savings-billions>.

# Efficiency

## IT Modernization and Cloud Adoption

Automating legacy system migrations and upgrades, optimizing resource allocation and infrastructure management, and providing advanced analytics can help accelerate modernization efforts and reduce costs in the transition to more cloud-based, agile, and scalable technologies.

Each year, the federal government spends more than \$100 billion on IT and cyber-related investments. Of this amount, agencies have typically reported spending about 80 percent on operations and maintenance of existing IT, including legacy systems.<sup>15</sup> The U.S. federal government uses many outdated systems and applications, some dating back over 50 years. These legacy systems are increasingly difficult to update, less interoperable, and prone to security risks, making modernization a complex and costly challenge. The process is often slow and seldom in lockstep with mission imperatives. Only a small number of agencies have modernized essential workflows, related applications, systems and data, across their organizations.

Progress toward modernization and cloud adoption has been limited by technical debt accumulated over years of budget shortfalls, a lack of diverse skills, and siloed computing platforms. Limited resources, complicated budget cycles, and bureaucratic decision trees hinder federal agencies' ability to modernize aging legacy systems and fragmented IT and data infrastructures, and to adopt the more efficient, secure, and scalable technologies needed to meet evolving demands and mission objectives.

Commercial strategies show a pathway to cost savings for government. A recent example is GSA's decision to partner with industry and consolidate all travel and expense into a shared service that will serve over 124 civilian agencies, more than a million federal travelers and over 2.6 million transactions a year. In addition, Oracle provides cloud-based ERP, supply chain management, payroll, and human capital management to over 100 federal customers—but this is just a start.

Many agencies rely on legacy code and mainframe applications that are difficult to maintain and integrate with modern technologies. These systems often harbor outdated applications and are difficult to scale, which prevents organizations from realizing their digital transformation goals. A key challenge is how to modernize years of development and operational work while keeping the lights on to serve the mission. Other common challenges include:

- **Antiquated Code Base:** Legacy applications are often built on a code base that was developed decades ago.

15. Highlights of GAO-23-106821, a testimony before the Subcommittee on Cybersecurity, Information Technology, and Government Innovation, Committee on Oversight and Accountability, House of Representatives.

- **Complexity:** Mainframe systems have complex architectures that are hard to document and analyze.
- **Talent Acquisition and Retention:** Languages such as COBOL and Assembly are not a common skill set for modern developers, so attracting and maintaining these resources is difficult.

As a recent report<sup>16</sup> on secure cloud adoption from the Center for Strategic and International Studies found that duplicative and obsolete legacy systems should be sunsetted wherever possible, and necessary systems should be replaced with modern technologies on more cost-efficient platforms.

Unfortunately, some agencies have operated massive projects that spin for years with no tangible results and limited accountability. This experience underscores the significance of avoiding costly modernization efforts that may not yield the expected outcomes. Instead, agencies should adopt cloud-based, scalable platforms and other proven modernization solutions to automate, streamline, and accelerate the IT and application modernization process, enhancing security while reducing operational costs.

Modernizing legacy IT systems requires investment. Successfully modernizing IT systems requires a return on that investment. As the federal government looks to make technology improvements, it needs to ensure accountability measures are in place within agencies and commercial partners tasked with implementing those changes. Returns should be measured and tracked over months and not years.

The IRS grapples with outdated IT systems and application code dating back to the 1960s. These legacy systems have resulted in data silos, hindering real-time processing and increasing operational costs due to the complexity of updating them as tax rules and policies evolve. In response to these challenges, the IRS has embarked on a modernization program based on best commercial practices, working with IBM and other industry partners. This has enabled the IRS to modernize its systems 300 percent faster than initially anticipated. This approach also leverages generative AI, cutting application code language translation processing time from 20 hours to 15 minutes. The resulting solution delivered more detailed business logic and more efficient functional code.

In addition, the DoD faced the challenge of maintaining an extensive enterprise network and supporting global business operations with outdated hardware and software systems. A Federal Systems Integrator approached Dell to transform the legacy network and modernize the entire enterprise platform in response to the looming end-of-support for Microsoft's Windows 2008. Dell's team collaborated with an enterprise architect to identify key requirements and develop a viable solution. The team proposed a transition to Azure Government Cloud, refactoring the existing management framework into a unified cloud control plane. A proof of concept was developed, allowing the government to assess vendor-based solutions. The solution enhanced operational flexibility and collaboration for warfighters, reduced login times significantly, and aligned with Zero Trust principles. It established a standard for a converged, defendable, and maneuverable architecture, improving network security and enabling scalable, efficient IT operations.

Modernization offers the promise of achieving more through improved productivity. For federal agencies, that promise can mean more agility, more efficiency and a greater chance of mission success. Through application modernization and adoption of secure

---

16. <https://www.csis.org/analysis/faster-cloud-federal-use-cloud-services>.



cloud platforms, agencies also have the potential to update the capabilities of existing applications to meet current technology standards, achieve faster resolution of issues, improve citizen services, and build trust. These examples are some reasons why application modernization is a key imperative for federal agencies across the government. Cost reduction opportunities from full implementation of these recommendations are estimated to be \$170 billion over 10 years.

Fortunately, AI provides new capabilities to help ease these challenges. From increasing developer productivity to accelerating application modernization and operational optimization, agencies can address many strategic outcomes in modernization projects. Adoption of generative AI can assist in modernizing legacy systems by tackling technical debt, bridging the skills gap, and enhancing developer productivity.

AI can assist in addressing common application modernization challenges, improve employee productivity and reduce costs. AI can support modernization in multiple ways, including:

- **Code assistants:** AI-powered code assistants can significantly enhance developer productivity and code quality. While AI accelerates development and modernization, human experts retain the final say in code approval and implementation. The combination of AI capabilities and human expertise can lead to more efficient modernization.
- **Tackling technical debt:** Technical debt, which includes outdated code, architecture, and documentation, can significantly hinder modernization efforts. AI can help by improving the classification of issues and generating code to resolve these issues. AI can enable context-sensitive automation to reduce time needed for code fixes. Using AI can also help with automating tasks like cloud infrastructure provisioning, patching, and maintenance, and accelerate code debugging and improved document generation.
- **Bridging the skills gap:** The shortage of federal in-house technical skills is a cross-agency challenge. AI can help address this by enabling code generation and translation, even for code unfamiliar to more recently trained developers, and summarizing and providing context for existing code, especially when original developers are unavailable. These and similar IT modernization actions will save millions of staff hours and prevent billions of dollars of underpayments.

In sum, application modernization and adoption of cloud computing are particularly critical, as many federal systems are outdated, some over 50 years old, making them difficult to update and secure. High costs, legacy technologies, and skills gaps present significant barriers to modernization. Accelerating the government's move to cloud native applications will provide better and faster security, flexibility, and data analytics.

## Cybersecurity

Investing in better cybersecurity systems and damage prevention will save significant resources for the government resulting from remediating damaging breaches.

The federal government's cybersecurity challenge is complex, urgent, and vulnerable to more advanced cyber adversaries who use AI and machine learning to launch greater volume, velocity, and sophistication of attacks. This progressing threat landscape poses a bigger danger given the challenges of legacy IT infrastructure, a shortage of skilled cybersecurity professionals, and the overwhelming volume of sensitive data that must be protected across the more porous boundaries of cloud and data sharing mission needs. The number of attacks on government and critical infrastructure have intensified by nearly 200 percent between 2021 and 2024, widening the gap in fortifying defenses against advancing technologies in the hands of adversaries.<sup>17</sup>

The 2024 Ponemon Cost of Data Breach study found the average total cost of a data breach has risen to \$4.88 million, a 10 percent increase over 2023 and the highest total ever.<sup>18</sup> Over the last eight years, data breaches by local, state and federal agencies have cost over \$26 billion. The U.S. Postal Service and the Office of Personnel Management had a combined nearly 82 million records compromised in the two largest all-government data breaches since 2014, according to the report compiled by Comparitech, a consumer-aid website that conducts research uncovering cybersecurity breaches.<sup>19</sup> Government budgeting efforts should acknowledge the ROI from cyber prevention over the spending needing by curing cyber incidents after the fact; cost efficiencies from these actions is estimated to affect \$500 billion over 10 years, largely in the form of reduced harm from cyber incidents. Of course, "harm avoided" does not "score" in governmental budgeting, making critical investments less likely as political considerations prevail.

The importance of strengthening and continuously fortifying effective cybersecurity technologies and best practices for government cannot be overstated. Data-rich, sensitive networks make agencies a prime target for increased espionage and disruptive attacks. Protections must evolve beyond existing defensive technologies and policies to include advancing government's detection and disruption techniques, driving greater accountability of commercial technology providers, and innovating workforce development with digital assistance and training.

- 1. Advancing government's detection and disruption techniques:** Applying recent advances in AI to cyber programs can automate threat detection, accelerate vulnerability remediation, detect intrusions in real-time, and continuously monitor for anomalous activity or emerging vulnerabilities. To do so, agencies should prioritize the development and deployment of AI-powered cybersecurity solutions to build

17. <https://blog.checkpoint.com/research/a-closer-look-at-q3-2024-75-surge-in-cyber-attacks-worldwide/>.

18. <https://www.ibm.com/reports/data-breach>.

19. [https://www.federaltimes.com/it-networks/2022/12/30/data-breaches-led-by-usps-opm-cost-governments-26-billion/#:~:text=Data%20breaches%20by%20local%2C%20state%20and%20federal,\\$26%20billion%2C%20according%20to%20a%20new%20report.&text=At%20OPM%2C%20hackers%20compromised%201.5%20million%20pieces,OPM%20and%20its%20contractor%20for%20affected%20employees](https://www.federaltimes.com/it-networks/2022/12/30/data-breaches-led-by-usps-opm-cost-governments-26-billion/#:~:text=Data%20breaches%20by%20local%2C%20state%20and%20federal,$26%20billion%2C%20according%20to%20a%20new%20report.&text=At%20OPM%2C%20hackers%20compromised%201.5%20million%20pieces,OPM%20and%20its%20contractor%20for%20affected%20employees).

scalable, adaptive systems and services that proactively help identify and mitigate cyber threats. Further, the ability to detect and disrupt a threat actor without launching into offensive activities means that the threat must be detected and contained within the perimeter of the breached environment. This requires a focus on containment or methods of disruption (e.g., disconnect affected systems, deny access, push policy on firewalls to block data movement), tools that enable visibility of the activities on a network, and tradecraft to impede the threat without hampering critical activities.

2. **Driving greater accountability of commercial technology providers:** In the past four years, technology providers accounted for a large vector of attack<sup>20</sup>—given their wide adoption across government and the private sector. Using technology and service providers as threat vectors to infiltrate U.S. government entities was effective in recent attacks on U.S. telecommunications and technology providers. While compliance with security standards like those from NIST<sup>21</sup> are already required, agencies should test their incident response plans with technology providers to drive escalation and containment strategies ahead of incidents. Findings could be applied towards contract requirements, emphasizing stakeholder responsibilities and evaluating future partnerships.
3. **Innovating workforce development with digital assistants and training:** AI has long been used in tuning the cybersecurity technology environment, but the emergence of generative AI—which can create new content and learn from patterns in existing data sets—enables security operators to augment skills, drastically improving productivity of time-consuming research or reporting tasks and enabling focus on prevention or remediation. The use of digital assistants also has the power to help users to self-train, augment playbook activities during alert investigations, and arrive at decisions more quickly—vastly reducing the time to detect and respond to threats.

Further, federal agencies and critical infrastructure organizations should participate in immersive cyber incident simulations. These simulations address challenges such as attacks on vital government services, communication breakdowns, and evolving government reporting requirements, while also showcasing demos on AI, threat detection, and hacking. By simulating high-pressure situations, the government's cyber teams can identify gaps in response plans, empowering them to defend against both current and emerging threats.

Organizations lacked the ability to distinguish between trustworthy and untrustworthy products in complex supply chain ecosystems, posing a cybersecurity risk. Dell collaborated with NIST to develop a prototype for verifying the integrity of computing devices within supply chains. The Secured Component Verification (SCV) capability was implemented to provide assurance of product integrity from the Dell factory to end-user delivery. The SCV allowed customers to verify components on-demand, reducing validation time and support costs. This guidance was incorporated into federal government procurement practices, enhancing cybersecurity and ensuring supply chain assurance for critical infrastructure.

---

20. <https://go.crowdstrike.com/rs/281-OBQ-266/images/GlobalThreatReport2024.pdf>.

21. <https://csrc.nist.gov/pubs/sp/800/53/r3/upd3/final>.

## IT Financial Operations (FinOps)

Through better management of financial operations, agencies can reduce up to 40 percent of current cloud spend, identify 5 percent of total IT budget for savings or redirection to high-priority technology investments, and generate an ROI of 10x over three years with an average break-even in month eight of service.

The Government Accountability Office (GAO) reports that federal agencies purchase approximately \$759 billion worth of contracts annually. Some encouraging news was reported in December 2024, when the Office of Management and Budget announced the use of Category Management to deliver over \$100 billion in savings and cost avoidance. This enterprisewide approach to federal contracting makes the government a more organized, better-informed buyer. Contracting reforms can strengthen the government's buying practices to ensure that tens of thousands of contracting officials get better deals on goods and services to deliver on agency missions.

Category management has proven to redefine efficiency in government procurement, ensuring that the federal government buys as an enterprise. These savings can be reinvested into critical programs, enhancing the delivery of public services while reducing taxpayer burdens. Category management exemplifies how smart policy and collaboration can drive meaningful change, ensuring the government operates more effectively and responsibly on behalf of taxpayers.

Decision makers across IT, finance, and the operational office lack financial accountability and transparency, leading to misinformation, incomplete data, and no means to directly link dollars spent to meaningful value and outcomes. Improving results in this area is possible, and cost efficiencies of up to \$150 billion over 10 years are achievable with effective implementation as demonstrated by three examples where IBM worked with national governments:

- A European government agency assessed and deployed FinOps services to maximize the value of its \$5-million cloud budget. This agency was able to implement a FinOps practice for managing ongoing cost and value, rapidly implementing optimization, and annualizing \$2.15 million in savings, with \$858,000 in savings delivered in the first five months—with a projected overall ROI of 248 percent over three years just on optimization of their cloud environment.
- In the U.S., one defense command leveraged FinOps to transform Planning, Programming, Budgeting, and Execution—resulting in transparent cost modeling, automated budgeting processes, improved data quality, and a reduction in budget variances by more than 20 percent.
- Another agency applied digital transformation and insights to \$9 billion in annual IT spend, decreasing budget variances to 1 percent during the fiscal year.



# APPENDIX: SCORING ADMINISTRATIVE SAVINGS

Specific rules govern how savings are "scored" in the federal environment. These rules are different than those used to calculate savings estimates in the private sector, and those leading reform initiatives must recognize some of the key distinctions.

Savings from reduced administrative spending can be scored if the President proposes and Congress enacts lower appropriations for agencies, signaling agencies to realize savings via operational reforms. Mandatory programs would have to follow a different but parallel process—agencies predictably resist such budget reductions for fear that efficiencies are "speculative." And lower budgets could ultimately reduce core functions and critical mission-related activities.

In the private sector, customers have found that administrative savings are consistently real and mission-enhancing. For government, this process could be implemented as follows.

The President's Budget would propose allocating overall savings targets to budget accounts for individual agency programs. Forecasted savings would be allocated among specific programs in the President's budget request.

Congress would then incorporate these savings targets into its annual Budget Resolution. Savings could be achieved in individual program accounts if Congress reduced the ceiling amount that agencies could spend for those programs in that year. Technically, this would reduce "budget authority" through a process known as "302" allocations. To score as savings, the annual Budget Resolution would have to allow appropriators to reduce the total 302(a) allocation for that year and subsequently reduce 302(b) allocations for individual programs to appropriations subcommittees; otherwise, the savings could simply be used for other discretionary spending within the total provided in the Budget Resolution. This would be a departure from the practice of using the budget resolution to specify a 302(a) top-line for appropriations, without instructions to the appropriators on how to allocate that to subcommittees or to achieve savings.

Both the Budget Resolution and subsequent appropriations legislation would have to include reductions consistent with the Fiscal Responsibility Act of 2023, which set caps on appropriations for fiscal years 2024 and 2025. It is unclear whether there will be caps pursuant to the reconciliation legislation now under consideration.

With less money allocated through the Budget, agencies would have to operate these programs more efficiently, through the proven means recommended in this report and/or other methods. If the administrative savings were not achieved, agencies would still have to reduce spending in other areas of the program to stay within their overall spending targets. Alternatively, allowing agencies to retain some portion of savings for discretionary use might create greater incentives for agency leadership to drive necessary change.

All of this would have to be tracked for each individual program for which savings was estimated, as well as at the aggregate level, to show savings relative to the previously established defense and non-defense caps. This could be a complex and lengthy process.

These steps would apply to all programs funded each year by the Budget, which are known as “discretionary” programs because Congress has discretion on whether and how much to appropriate.

For “entitlement” programs such as Medicare, a portion of the administrative costs are funded out of the overall amount collected to operate the program, as opposed to annual appropriations. These are known as “mandatory” programs, because the spending is “mandated” based on how many services participants use and how much those services cost. Reductions in mandatory spending, such as savings in improper payments identified in this report, can be scored if legislated changes to the authorities for those programs mandate the actions that produce these savings. The savings would be scored over a multiyear period, reflected in reduced spending estimates for those programs. For this to occur, the budget resolution would provide instructions to authorizing committees to ensure achievement of specified amounts that can be used to achieve scorable savings.

In the longer term, the administration could work with Congress to develop consistent scoring rules for multiyear savings. Under existing rules, CBO would incorporate the impacts of current investments in baseline estimates but would not normally include the changes in the legislation enacting new investments that would have future-year impact. As described above, much of the savings would arise in discretionary accounts subject to annual appropriation. Future appropriations could be lower, but under existing rules Congress could not claim any of the savings for current initiatives because the appropriation bill covers only the current year. CBO has generally viewed proposed out-year savings from administrative investments and reforms skeptically, absent strong evidence that these savings will be achieved. However, the administration could work with Congress to enact process changes that allow appropriators to get credit for savings achieved beyond the budget year. Allowing agencies to count savings over multiple years is more consistent with how capital accounting for IT-enabled savings is done in the private sector.



# CONCLUSION

This report underscores the critical need for the U.S. federal government to modernize its IT infrastructure and adopt innovative technologies to enhance efficiency and reduce costs. Highlighting the substantial budget challenge and the outdated nature of many federal systems, the report presents a comprehensive roadmap for achieving \$2 trillion in cost reductions and efficiency improvements over the next decade. These effects are projected through various initiatives such as fraud prevention, artificial intelligence, IT modernization, and cybersecurity improvements. The report emphasizes that these recommendations are not merely theoretical, but based on proven successes in both the public and private sectors. The potential benefits extend beyond financial savings, promising improved security, reliability, and service quality for the American public.

Incorporating industry best practices and prioritizing implementation to ensure timely and effective execution of the proposed initiatives is in the best interest of the federal government and citizens. This report demonstrates how modern technologies and the collective experience of industry leaders can support the transition to a more efficient and modern federal IT environment. By adapting the strategies described here, the government can not only reduce costs but also drive productivity, innovation, and efficiency to better serve the American people.

# REFERENCES

1. GAO Reports (GAO-22-105301, GAO-24-107660): This report discuss federal savings through Robotic Process Automation (RPA) and shared services, respectively.  
<https://www.gao.gov/products/gao-22-105301>.
2. FedScoop Article: This article highlights RPA savings for federal agencies.  
<https://fedscoop.com/rpa-savings-federal-agencies-reinvest-suzette-kent/>.
3. CIO.gov Policy Paper: This document discusses federal shared services.  
[https://assets.cio.gov/assets/files/resources/SOFIT-Policy-Papers\\_D\\_FederalSharedServices\\_PR\\_v2.pdf](https://assets.cio.gov/assets/files/resources/SOFIT-Policy-Papers_D_FederalSharedServices_PR_v2.pdf).
4. IBM News Release: IBM receives FedRAMP authorization for its federal human resource shared services solution.  
[https://newsroom.ibm.com/2023-08-30-IBM-Receives-FedRAMP-Authorization-for-its-Federal-HR-Shared-Services-Solution?mhsrc=ibmsearch\\_a&mhq=Federal%20Shared%20Services](https://newsroom.ibm.com/2023-08-30-IBM-Receives-FedRAMP-Authorization-for-its-Federal-HR-Shared-Services-Solution?mhsrc=ibmsearch_a&mhq=Federal%20Shared%20Services).
5. Additional GAO Reports: This reports touches on various aspects of federal spending and operations.  
<https://www.gao.gov/products/gao-24-107660>.
6. CBO Reports: This report discusses federal budget topics, including technology investments.  
[https://www.cbo.gov/publication/61147#\\_idTextAnchor000](https://www.cbo.gov/publication/61147#_idTextAnchor000).
7. Kiplinger Article: This article explores how AI catches tax cheats and saves billions.  
<https://www.kiplinger.com/taxes/treasury-ai-catching-tax-cheats-and-savings-billions>.
8. GAO Testimony: This testimony discusses cybersecurity and IT modernization in government. Highlights of GAO-23-106821, a testimony before the Subcommittee on Cybersecurity, Information Technology, and Government Innovation, Committee on Oversight and Accountability, House of Representatives
9. Cybersecurity Reports: These reports highlight global cyberattack trends and data breaches, including those affecting USPS and OPM.  
<https://blog.checkpoint.com/research/a-closer-look-at-q3-2024-75-surge-in-cyber-attacks-worldwide/>.

<https://www.ibm.com/reports/data-breach>.[https://www.federaltimes.com/it-networks/2022/12/30/data-breaches-led-by-usps-opm-cost-governments-26-billion/#:~:text=Data%20breaches%20by%20local%2C%20state%20and%20federal,\\$26%20billion%2C%20according%20to%20a%20new%20report.&text=At%20OPM%2C%20hackers%20compromised%201.5%20million%20pieces,OPM%20and%20its%20contractor%20for%20affected%20employees.](https://www.federaltimes.com/it-networks/2022/12/30/data-breaches-led-by-usps-opm-cost-governments-26-billion/#:~:text=Data%20breaches%20by%20local%2C%20state%20and%20federal,$26%20billion%2C%20according%20to%20a%20new%20report.&text=At%20OPM%2C%20hackers%20compromised%201.5%20million%20pieces,OPM%20and%20its%20contractor%20for%20affected%20employees.)

<https://go.crowdstrike.com/rs/281-OBQ-266/images/GlobalThreatReport2024.pdf>.

10. This reports covers application modernization, hybrid cloud solutions, and trusted AI governance.

<https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/application-modernization-hybrid-cloud>.

11. IBM IBV Report: This report explores the power of AI in security.

[The Power of AI: Security.](#)

12. IBM Center for The Business of Government Report: This report examines AI and the modern tax agency.

[AI and the Modern Tax Agency.](#)

13. White House Press Release: This release discusses a prepared federal government, preventing fraud and improper payments.

[A Prepared Federal Government: Preventing Fraud and Improper Payments in Emergency Funding.](#)

14. IBM Developer Blog: This blog post outlines nine ways developers can benefit from AI assistants.

[Nine Ways Developers Can Benefit from AI Assistants.](#)

15. These reports discuss AI in human resources and talent acquisition. These resources cover a wide range of topics, including IT modernization, AI governance, cybersecurity, and the application of AI in various government functions, such as human resources and payment integrity.

[Artificial intelligence and a new era of human resources](#)

[The CEO's Guide to Generative AI, What is AI Governance?](#)

[Navigating Generative AI in Government](#)

[Better Citizen Experiences with generative AI Chatbots.](#)

TECHNOLOGY CEO  

---

COUNCIL

1341 G Street NW, Suite 1100

Washington, DC 20005

202.585.0258

[info@techceocouncil.org](mailto:info@techceocouncil.org)