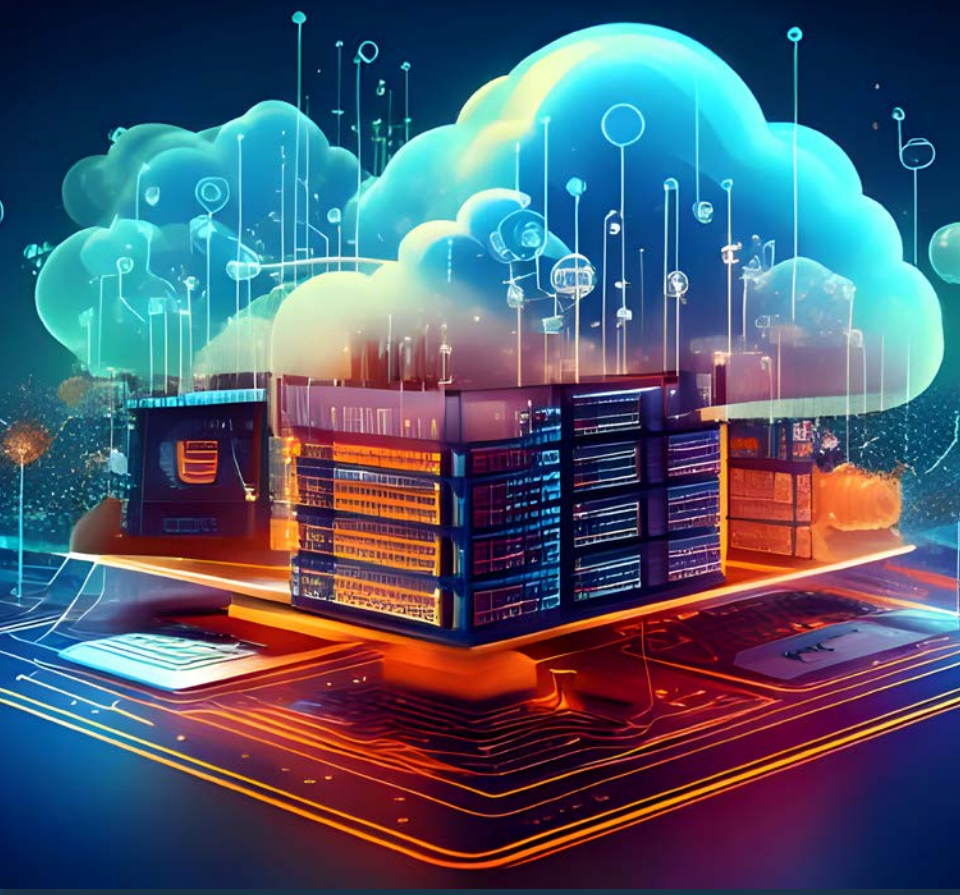
IBM Center for The Business of Government 2025



How **TECHNOLOGY** Can Drive **GOVERNMENT EFFICIENCY**

IBM Center for The Business of Government

Table of Content

FOREWORD

In an era marked by unprecedented technological advancements and fiscal challenges, the imperative for the U.S. federal government to modernize its operations has never been more critical. This is highlighted by a recent report, led by the Technology CEO Council (TCC), in which the IBM Center for The Business of Government participated. That report, *How Productivity, Innovation, and Efficiency Can Transform American Government*, details how, if implemented effectively, technology-based reforms could reduce federal costs significantly—now and over time.

This report, *How Technology Can Drive Government Efficiency*, is a companion piece to the more detailed TCC report and discusses leveraging IT modernization, business process innovations, and artificial intelligence (AI) to transform government operations—leading to improved service quality and lower costs. The insights and recommendations contained within this report are grounded in real-world experiences from both the public and private sectors, adapted to address the significant scope of the federal government.

This report identifies several key areas for improvement, including fraud and improper payments prevention, AI, IT modernization, the use of common systems for common purposes, and financial operations. The potential benefits also include improved security and reliability from government for the American public. The recommendations provide a roadmap for federal agencies to meet their missions more efficiently, at a lower cost, and with reduced risk.

The report demonstrates that: through strategic investments in technology and a commitment to continuous improvement, agencies can transform operations to better serve the needs of the nation.

Daniel J. Chenok
Executive Director
IBM Center for
The Business of Government
chenokd@us.ibm.com

INTRODUCTION

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.

Prior studies have suggested cost savings opportunities approaching this estimate. The Government Accountability Office (GAO) issued a 2022 report that identified savings opportunities in the tens of billions of dollars range from 94 separate actions.[1] 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.[2]

Achieving this level of savings and efficiency will necessitate technology adoption to promote effective government operations.[3] For example, in 2019 U.S. Chief Information Officer (CIO) Suzette Kent cited significant savings from robotics process automation.[4] 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. The recommendations in this report can help the government to adapt commercial practices to help agencies achieve the benefits of modernization.

COST EFFICIENCY OPPORTUNITIES

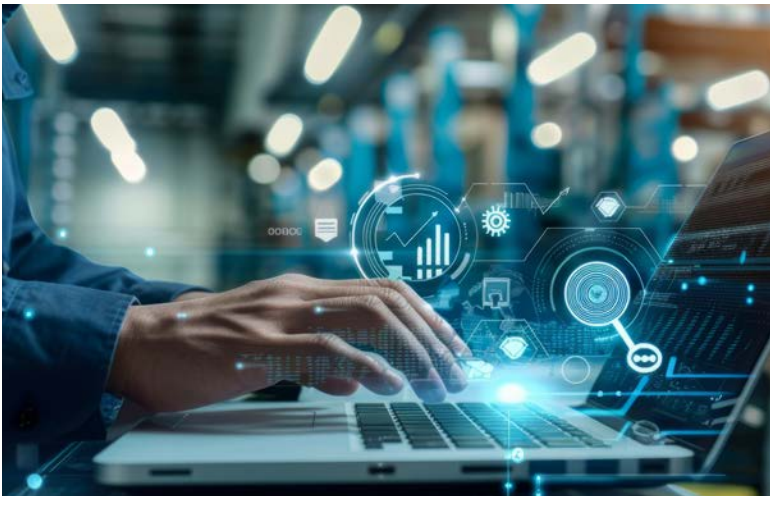
Integrating Common Systems Through Shared Services

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.

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 reinvent 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. By focusing on existing providers, agencies can capitalize on the expertise and investments in innovation to maximize the advantages of shared services.

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

Enhance Mission Focus: Agencies become more productive, avoiding focus on backoffice 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.

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.

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.

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 reported[5] 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.[6]

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.

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[7] 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.

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 government 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.

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.

Today's most successful organizations 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.

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 government 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.[8] AI technologies can also increase developer productivity, supporting modernization of old systems and bridging the skills gap between government and industry.

There are abundant opportunities for AI-driven transformation of critical federal government programs to enhance efficiency, strengthen citizens' trust in government, and bolster security.

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:

- 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.[9]

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.[10] 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.

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.
- **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[11] 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.

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 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.

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, such as increasing developer productivity, modernizing technical debt, and supporting decision making.

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 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.[12] 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.[13]

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 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[14]—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[15] 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.

IT Financial Operations (FinOps)

Through better management of financial operations, agencies can reduce current cloud spend and redirect savings to high-priority technology investments.

The Government Accountability Office 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 enterprise-wide 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.

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 roadmap for achieving 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 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 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 https://www.gao.gov/products/gao-22-105301.
2 https://www.mckinsey.com/industries/public-sector/our-insights/us-government-productivity-a-more-than-2000-per-resident-opportunity.
3 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.
4 https://fedscoop.com/rpa-savings-federal-agencies-reinvest-suzette-kent/.
5 https://www.gao.gov/products/gao-24-107660.
6 https://www.gao.gov/products/gao-24-107660.
7 https://www.businessofgovernment.org/report/enhancing-government-payment-integrity-leveraging-ai-and-other-emerging-technologies.
8 https://www.cbo.gov/publication/61147#_idTextAnchor000).
9 https://www.cbo.gov/publication/61147.
10 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.
11 https://www.csis.org/analysis/faster-cloud-federal-use-cloud-services.
12 https://www.ibm.com/reports/data-breach.
13 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%2021.5%20million%20pieces,OPM%20and%20its%20contractor%20for%20affected%20employees.
14 https://go.crowdstrike.com/rs/281-OBQ-266/images/GlobalThreatReport2024.pdf.
15 https://csrc.nist.gov/pubs/sp/800/53/r3/upd3/final.

About the IBM Center for The Business of Government
Through research stipends and events, the IBM Center for The Business of Government stimulates research and facilitates discussion of new approaches to improving the effectiveness of government at the federal, state, local, and international levels.

About IBM Consulting
With consultants and professional staff in more than 160 countries globally, IBM Consulting is the world's largest consulting services organization. IBM Consulting provides clients with business process and industry expertise, a deep understanding of technology solutions that address specific industry issues, and the ability to design, build, and run those solutions in a way that delivers bottom-line value. To learn more visit ibm.com.

For more information:
Daniel J. Chenok
Executive Director
IBM Center for The Business of Government

600 14th Street NW
Second Floor
Washington, D.C. 20005
202-551-9342

IBM Center for The Business of Government