opentext™

Enabling smarter government with cloud-based information management

How public sector CIOs can address multiple EO mandates with a single platform

"With OpenText, we see a significant improvement in our efficiency, allowing us to investigate more complaints and bring more offenders to justice."

– Allen LaFontaine
Forensics Examiner, Southern Alberta Internet Child Exploitation Unit

Industry backdrop

Public sector CIOs are painfully familiar with the concept of high accountability and low authority. They are expected to keep up with private sector advances around digitization, application modernization, customer experience, artificial intelligence and cloud migrations, while also securing citizen data against cyberattacks. In the meantime, CIOs are budgetarily handcuffed, with more government IT funding needed to effectively maintain outdated systems. This results in a long CIO fix-it list with scarce funding to get things done.

There is an urgent need to flip this concept around and provide government CIOs with a way to do more for less, to take control of their destiny and set their agency on a course for rapid transformation. This paper details how agencies around the globe are taking a smarter approach to government IT and how getting citizen and public sector information AI-ready delivers significant security, automation and modernization benefits.

OpenText vision: AI and automation at scale

US federal agencies must comply with various executive orders (EO) signed by the president and overseen by the Office of Management and Budget (OMB). These orders include guidance on cybersecurity, federal customer experience, infrastructure and artificial intelligence. In addition, the OMB has issued a series of memoranda requiring government agencies to meet certain criteria tied to digital accessibility standards, privacy management, electronic records requirements and software supply chain security.

To comply with these orders, each department will identify projects related to employee experience, citizen experience, application modernization, network security, application security, IT operations, AI and content management. Each of these projects must wait to be funded individually, and each one brings its own set of integration headaches.

This approach is time-consuming and costly, and most importantly, it is not working. Government lags behind the private sector regarding customer satisfaction scores and the number of workloads migrated to the cloud. At the end of each year, CIOs are often faced with a longer to-do list than at the beginning of the year.

Leveraging cloud-based information management, smarter government agencies can comply with executive orders and OMB memoranda while modernizing applications, strengthening cybersecurity, digitizing records, providing exceptional citizen experience and migrating more workloads safely to the cloud.

By using content management tools in a way that makes agency information "genAI-ready," a simple query can derive insights from complex documents without compromising security or compliance. As a result, smarter agencies can gain insights from structured and unstructured data and video and audio files using AI at massive scale.

In addition, smarter agencies can accomplish more by adopting a platform that can address many of their needs with smoother integrations at lower total cost. And that lets government focus on its bottom line—the mission.

Smarter information creates smarter governments

By partnering with a trusted software provider that can support multiple executive orders and OMB memoranda, governments can work smarter via:

- Smoother integrations with existing enterprise IT systems
- Faster time to benefits
- Lower overall cost
- More efficient maintenance and operations

With a cloud-based information management platform, agencies can connect, manage and extract analytical value, tapping into the power of AI, empowering modern work and better managing information for any type of user or experience. And the impact is broad, with smarter information powering smarter governments to drive value in multiple ways.

Delivering a total citizen experience

To meet citizen expectations, **EO 14058 "Transforming Federal Customer Experience"** recommends that agencies provide a personalized, self-service interface where citizens can find user-specific information, including status updates for pending items, such as a license renewal, grant application or a required quarterly business submission.

Effective information management allows agencies to offer additional personalization, also providing tailored notifications to citizens and businesses, such as emergency notifications and instructions for localized weather events.

In addition, agencies can push audio and video information out on social media and provide online portals to help citizens get the information they need without having to navigate departments and bureaus within an agency.

Plus, government agencies can provide multichannel chatbots and call centers, all operating off the same information, even using an AI-powered chatbot to address basic inquiries.

These IT efforts help deliver a citizen experience that provides timely, useful, tailored information in real time, meeting rising consumer expectations for speed and personalization.

Protecting against public sector cyber threats

Government computers and networks are a critical path to sensitive data and are central to operations. Malicious access and unauthorized changes to these systems can have a significant impact on an agency's operations and, potentially, that of the country.

The global cybersecurity market has been growing at a rate of 11 to 12 percent over the past several years.[1] The zero trust security model, entering its fourth year since the National Institute of Standards and Technology's (NIST) Special Publication 800-207, is widely adopted globally, proving to be a solid framework to secure government data and infrastructure.

1 Wall Street Journal, Cybersecurity Budgets Grow, But at a Slower Pace. September 2023

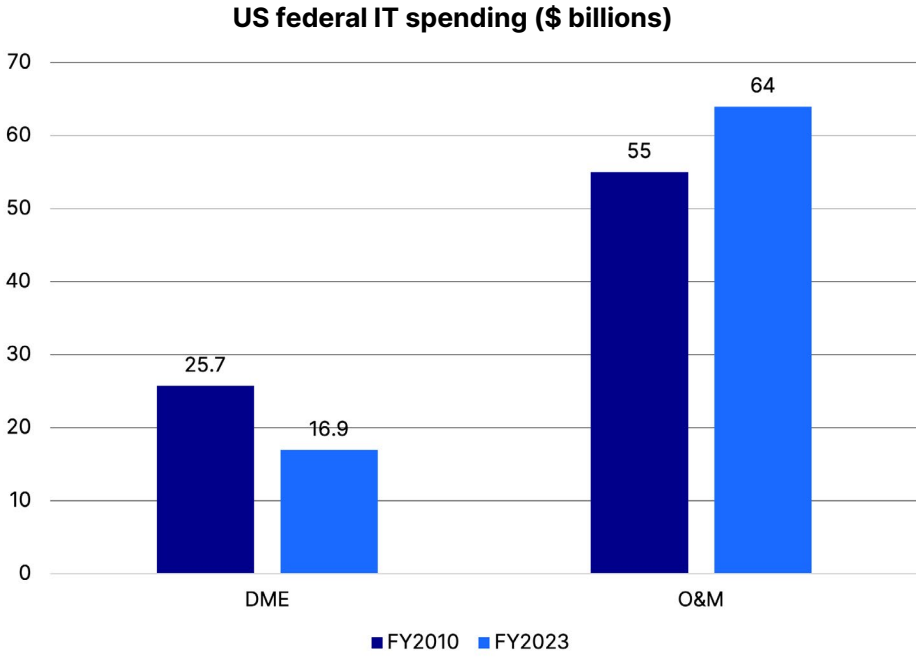
EO 14028 "Improving the Nation's Cybersecurity" calls for eight technology mandates, including implementing a NIST-oriented zero trust architecture, enhancing software supply chain security and improving vulnerability detection on federal networks.

Smarter governments take a holistic approach to cybersecurity, leaning on tools that provide detection, response and remediation in a zero trust environment.

Modernizing legacy systems

Government IT systems have not kept pace with changing organizational needs and are quickly becoming obsolete. In terms of the continued government dependency on legacy systems, GAO has declared this area "high-risk" and identified 10 critical systems that are severely outdated. Two of these are more than 50 years old, dating back to the Lydon B. Johnson administration.

These legacy systems not only pose a critical threat to their mission success, they also carry a huge operation and maintenance burden, slowing a culture of innovation. By far the biggest burden for federal IT budgets is operations and maintenance costs, making up more than 79 percent of all federal IT spending in FY 2023,[2] leaving relatively little spend for new development.



OMB Memoranda 23–07 requires federal agencies to fully digitize permanent records by June 2024. Smarter governments are able to scan in all paper records using AI, so that each file is automatically categorized and entered into the appropriate workflow environments. Smarter agencies limit data entry and manual steps wherever possible.

Smarter governments are also able to modernize legacy apps with low code or no code applications, to save time and money and make it easy to modify when necessary. They also take a strategic approach to archiving that allows them to have access to all the critical information without having to keep a legacy app going just to have the data on hand.

2 Statista, Federal government information technology (IT) expenditure in the United States from FY 2011 to FY 2023, by significance.

Enabling a hybrid workforce

A hybrid government workforce has pushed government to provide employees secure access to all the relevant files they need, whether logging on from home, an office location or a coffee shop.

Smarter government CIOs have deployed a comprehensive IT service management structure that allows for automatic and fast troubleshooting and self-help, with an intuitive interface requiring little to no employee training.

Smarter governments also provide an identity and access control system to make sure that information is only available to employees who have a need to review those data.

Tapping into AI and data analytics

Public sector IT departments face a continual increase in the volume of data to absorb and analyze. This data is also growing more complex, as unstructured video and audio files proliferate and more agencies deploy sensors as part of their IoT strategy. By making data more actionable, smarter government organizations can make effective, more informed decisions while enforcing security, privacy and regulations compliance. By reducing the time spent tracking down needed documents, agencies can improve citizen response times, boosting trust and worker morale.

Smarter governments are following the guidance from **Executive Order 14110 "Safe, Secure and Trustworthy AI,"** deploying AI tools to identify trends and generate actionable intelligence. Federal agencies have centered their missions around helping the most vulnerable populations, and AI is key to ensuring that each program is effectively sending help where it's needed most.

Smarter agencies provide tools to oversee software developers to ensure that red flags are identified early in the development process to avoid building products that miss the mark.

In addition, the use of eDiscovery tools allows agencies to quickly find information relevant to a specific legal matter. Likewise, intelligent FOIA search tools follow government rules regarding what's excepted and what must be disclosed, lowering agency risk.

Accelerating cloud migrations

Cloud migrations can help the public sector enhance innovation, reduce costs and improve security. Smart agencies are making cloud an important part of their Environmental, Social and Governance strategy. In a recent OpenText survey, 150 public sector respondents agreed the cloud was important to support a remote workforce, cost savings and better security.[3] But despite these benefits, the public sector continues to lag behind commercial firms in cloud migrations.

Many public sector CIOs still see data security in the cloud as an inhibitor, and that's why programs like FedRAMP are so important to provide confidence around cloud deployments. Smarter government CIOs deploy FedRAMP-authorized solutions to ensure compliance, security and establish faster cloud deployments.

3 Center for Digital Government for OpenText, Cloud Migration Survey. 2021

Why OpenText

OpenText is trusted by the Top 20 national governments around the world to address critical IT needs and public sector mandates under a single umbrella. OpenText is trusted by industry experts, with analysts recognizing us as a leading provider in categories including e-discovery solutions, customer communications management, supply chain networks and applications security.

As a member of the Joint Cyber Defense Collaborative, a public-private partnership housed within the Cybersecurity and Infrastructure Security Agency, OpenText is assisting the US government and its allies in the areas of threat intelligence and insights.

Proposed next steps

Together, we can outline a vision and identify opportunities to address your agency's technology plans. Below are suggested next steps.

- **Introductory meeting:** Bring together your OpenText Senior Account Representative with your organization's technology and/or mission bureau leaders.
- **Engage the OpenText Professional Services team:** Assess your state of readiness and define a vision and roadmap to optimize your modernization approach.

Keith Nelson

Senior Industry Strategist, OpenText Public Sector

Email: nelsonk@opentext.com

LinkedIn: Keith Nelson