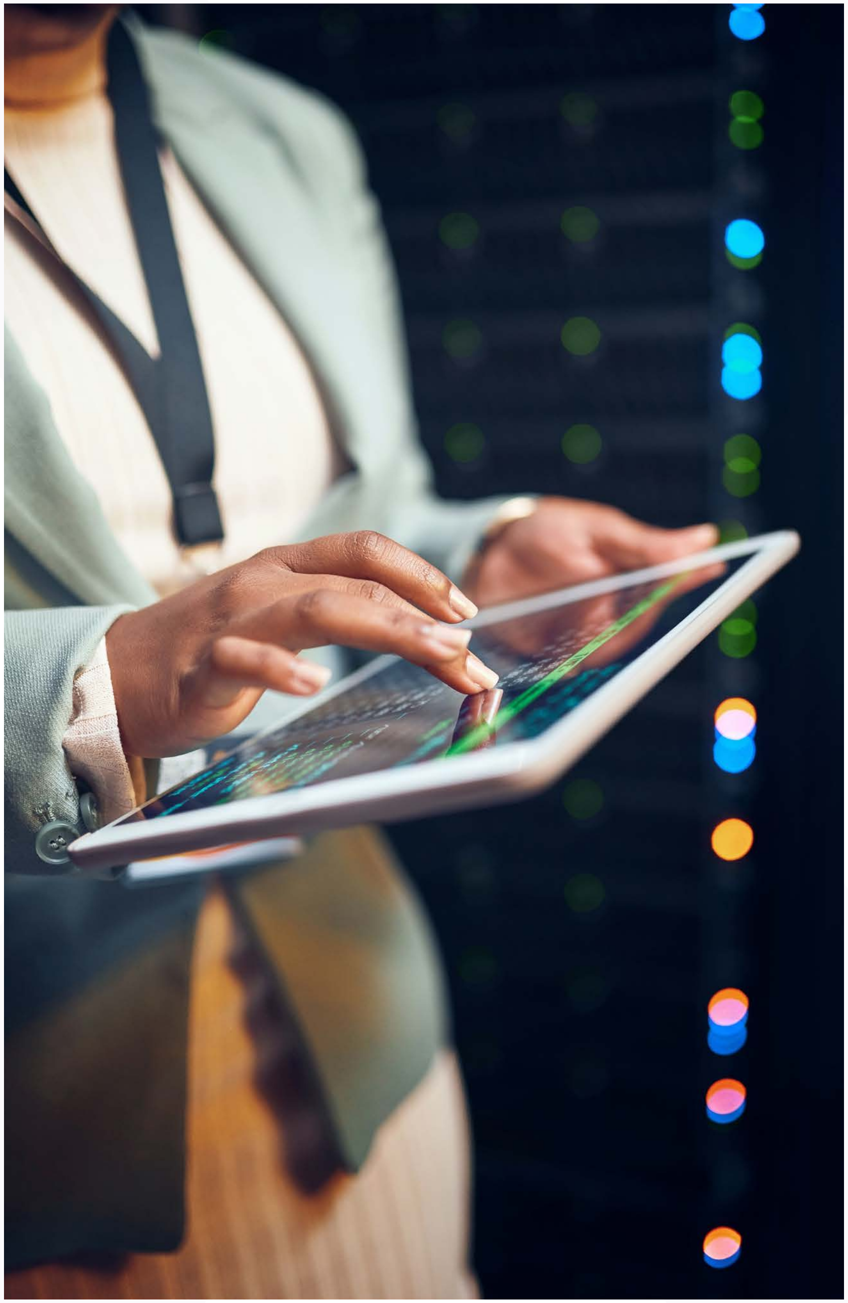
Accelerating mission success with AI-powered digital transformation

Insights for federal leaders on the strategic and responsible use of AI for transformation

maximus



INTRODUCTION

The future of artificial intelligence (AI) in the public sector holds incredible promise, with the potential to redefine how government agencies operate, deliver services, and safeguard public trust. AI's promise extends beyond efficiency gains; it can unlock actionable insights for improved decision-making, elevating mission impact. However, achieving these outcomes requires more than adopting cutting-edge technology. Federal agencies must establish the right technical controls, measures, and governance frameworks to ensure AI solutions are secure, scalable, and aligned with public sector priorities.

The groundbreaking Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, issued in late 2023, followed by Office of Management and Budget (OMB) Guidance for Agencies and the National Institute of Standards and Technology (NIST) AI Risk Management Framework (RMF) in the spring, are setting the stage for AI to transform government operations. What federal leaders need now are actionable strategies to achieve these objectives, drive AI modernization, and protect against advanced cyber threats in an increasingly digital world.

Responsible AI use involves implementing ethical guidelines, ensuring transparency, and maintaining accountability in AI systems. Prioritizing responsible AI enables federal agencies to harness the full potential of AI while mitigating risks, fostering public trust, and ensuring that AI advancements benefit society as a whole.

CHAPTER ONE: AI AND DIGITAL TRANSFORMATION

Each year, the federal government serves more than 400 million individuals, families, businesses, and organizations, the majority of whom access those services via the internet. As the government continues to prioritize "simple, seamless, and secure" digital services and harness the power of AI across agencies, significant potential for digital transformation lies at the intersection of those two goals.

"Digital includes applications, operations, and customer experience – it is everywhere," explains Raymond Holder, managing director of digital growth at Maximus. He notes that when it comes to modernization, government clients are looking for ways they can use AI and machine learning (ML) to "accelerate application development, streamline operations, and ultimately improve customer and employee experience."

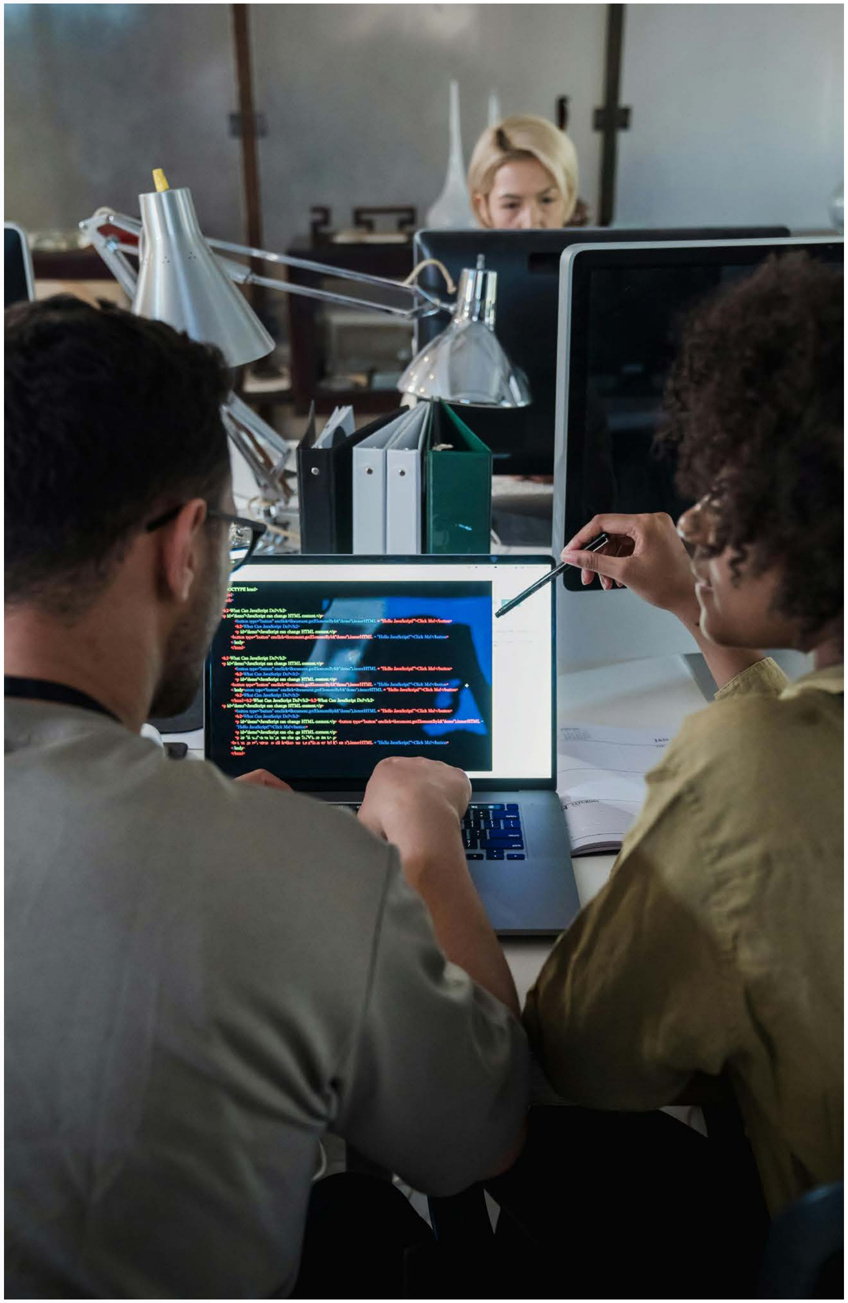
Developing a clear AI implementation roadmap is essential, given the range of possible use cases. Begin by identifying the desired mission outcomes, then work with AI experts to determine the necessary solutions. Shown below are examples of how AI can enhance mission impact.

AI Use Case Examples

- Customer Experience
- Workflow Optimization
- Supply Chain
- Fraud Detection
- Operations Management
- Data Discovery
- Content Support
- Digital Assistant

But no matter how it will be used, it is crucial to maintain responsible human oversight to ensure ethical and effective AI deployment.

While AI manages routine tasks, humans remain actively involved in decision-making, monitoring, and intervening when necessary. This approach ensures that AI systems operate within ethical guidelines, maintain transparency, and are accountable for their actions.



By balancing automation with human oversight, agencies ensure that AI advancements align with public interest and trust.

"There are many interesting and sophisticated use cases for AI," states Frank Reyes, managing director of software and infrastructure capabilities at Maximus. "But a really impactful one is just getting low-level, mundane tasks automated with a bit more intelligence and out of the way so people can really focus on the more humanistic critical and creative thinking."

AI use cases for government

Streamlining workflows. Federal workflows are often slowed by the siloed, dispersed nature of federal data – even within agencies and departments. Data related to a single individual, for example, may exist in numerous variations. Robert Smith, Bob Smith, B. Smith, R. Smith could all refer to the same person. Automated tools are key to reconciling these differences and completing tedious, time-intensive tasks much faster.

Enhancing customer experience. Improving customer experience across government remains a key priority. With 400 million annual customers, the federal government has plenty of feedback to tap into. The bigger challenge is gleaning actionable insights from vast amounts of data. Here, AI, via sentiment analysis, assists agencies in processing the data. Sentiment analysis taps into natural language processing (NLP) and ML to analyze feedback, picking out trends pertaining to how customers feel about the quality of services, products, and interactions.

Topic modeling is another NLP-based approach to understanding customers' requirements. It analyzes text for frequently used words or phrases, then presents a statistical breakdown of usage – identifying what customers are talking about the most. Regular topic modeling enables agencies to enhance the dynamism of their websites and other digital offerings.

By understanding customer sentiment, agencies can leverage customers' own voices and expectations to guide the design and delivery of government services to best meet their needs. AI-driven sentiment analysis and topic modeling gather and organize this data significantly faster than traditional methods, such as user surveys.

Optimizing software development. AI-powered code analysis helps federal technologists quickly identify errors, security risks, and areas for improvement. It gives them a clear view of their code landscape and helps them plan for future updates. This approach allows for gradual changes rather than jumping straight into the deep end of AI.

"AI is revolutionizing code development by automating repetitive tasks, enhancing code quality, and accelerating the development process," explains Kathleen Featheringham, vice president of artificial intelligence, Maximus. "As we look to the future, AI will become an indispensable support tool, enabling developers to focus on creative problem-solving and innovation while AI handles the heavy lifting of code generation, debugging, and optimization."

This offers significant opportunities for federal agencies that have faced technology workforce shortages for years. AI enhances human abilities rather than replacing them, allowing government employees to accomplish more, explore new possibilities, and drive innovation by automating routine tasks.

By reducing technical barriers and simplifying the coding process, agencies can envision a future where government analysts, even without advanced technical backgrounds, develop the necessary skills to effectively utilize AI in creating the tools they need. This approach alleviates the burden on limited government IT staff.

> **"As we look to the future, AI will become an indispensable support tool, enabling developers to focus on creative problem-solving and innovation while AI handles the heavy lifting of code generation, debugging, and optimization."**
>
> **KATHLEEN FEATHERINGHAM, VICE PRESIDENT OF ARTIFICIAL INTELLIGENCE, MAXIMUS**

> **“Government and industry partnerships are key to driving innovation. Industry partners provide an environment for government to evaluate these new technologies and processes securely, to test and learn as well as co-create, because that’s really the key.”**

RAYMOND HOLDER,
MANAGING DIRECTOR OF
DIGITAL GROWTH, MAXIMUS

Laying the foundation for AI implementation

Holder encourages government customers to begin by asking a series of basic, yet critical questions to ensure they are aligning with the mission, understanding target customer segments and their ideal outcomes, as well as identifying potential challenges for achieving AI implementation success.

“I call them ‘gain achievers’ or ‘pain relievers’ — once you identify what those things are, you can work backward to determine where AI and machine learning can be implemented for automation. Or where AI can be used to interact in new ways,” Holder explains.

While technology will evolve, certain aspects of the mission and strategy will remain constant, he adds. Compliance will always be a concern, as will enhancing security, agility, and resilience. Regardless of the new technology, from Big Data to cloud and now to AI, those fundamental needs remain. This serves as a starting point, alongside seeking and evaluating partners that will streamline the path to mission success.

“Government and industry partnerships are key to driving innovation. Industry partners provide an environment for government to evaluate these new technologies and processes securely, to test and learn as well as co-create, because that’s really the key,” Holder points out. “Setting up an environment where you can separate a particular set of data, interact with a particular set of customers or evaluate a specific use case, so that you can iterate and learn, is critical.” Agency leaders and industry partners can work together to establish a broad vision for AI in the agency, collectively creating an interconnected architecture that integrates these models into a cohesive digital ecosystem.

“Leveraging AI engineering to connect diverse AI models within unified workflows enables the scalable use of AI, significantly reducing the need for custom integration,” Featheringham notes. “This approach not only streamlines deployment but also facilitates active monitoring and management, ensuring that AI systems remain efficient, adaptable, and aligned with organizational goals.”

CHAPTER TWO: THE ROLE OF AI IN CYBERSECURITY AND CLOUD

As federal agencies progress on their digital modernization journeys, AI will be a critical tool in optimizing cloud and cybersecurity management. Increasingly, agencies are moving applications and operations to the cloud to achieve greater flexibility, reliability and scalability. However, this shift increases attack surfaces, making robust cybersecurity more crucial than ever.

In April 2024, the National Security Agency published the "Joint Guidance on Deploying AI Systems Securely," in collaboration with cybersecurity agencies in Australia, Canada, New Zealand, and the United Kingdom. The document highlights the importance of updating AI systems in the face of increased attack sophistication and changing risk profiles.

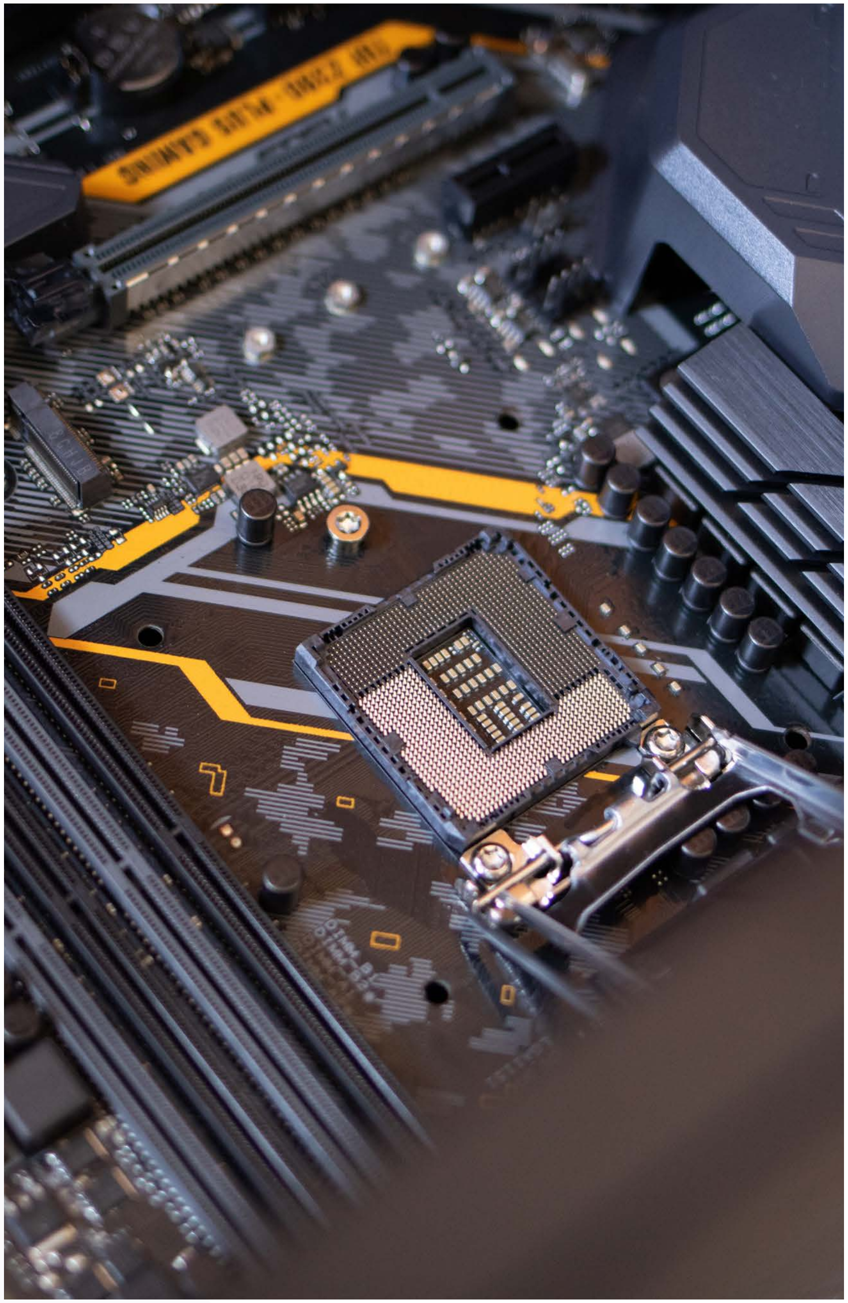
The document underscores AI as a human-machine partnership – a relationship of checks and balances. It states that while automation can make "IT and security teams more efficient by giving them insights that enable quick and targeted reactions to potential cyber incidents," it's also important to "carefully weigh the risks and benefits and ensure there is a human-in-the-loop where needed." Simultaneously, humans can introduce risks or vulnerabilities that AI can help mitigate.

"Around 88% of data breach incidents are user driven. It's inevitable that humans will make mistakes," states Kynan Carver, managing director of cybersecurity at Maximus. "By integrating AI and machine learning technologies to support individuals in their work, we can significantly reduce the number of incidents."

What AI brings to the cloud

Though cloud platforms have provided AI capabilities for some time now, sophisticated machine learning and deep learning capabilities are making it easier to implement AI "without having such a deep bench of in-house expertise," Reyes notes.

Cloud-based AI services automatically provision, deploy and manage cloud resources and applications within minutes. Based on predicted



> “Around 88% of data breach incidents are user driven. It’s inevitable that humans will make mistakes. By integrating AI and machine learning technologies to support individuals in their work, we can significantly reduce the number of incidents.”
>
> KYNAN CARVER, MANAGING DIRECTOR OF CYBERSECURITY, MAXIMUS

demand and usage patterns, those resources are able to scale as needed, optimizing use, performance, and cost.

“Major cloud service providers (CSPs) are now offering pre-trained models and customizable AI services, including natural language processing, image recognition, and predictive analytics,” Reyes explains. “CSPs have not only been utilizing these services for their own internal operations, but they are now expanding these capabilities to offer them to customers and users.” These low-code/no-code (LCNC) solutions help accelerate the development and deployment of machine learning models.

In a federal landscape increasingly adopting hybrid and multi-cloud architectures – integrating on-premises, private, and public cloud services from various CSPs – the resulting spread of data and applications across platforms and service providers can create significant complexity. In this context, AI becomes a transformative force within multi-cloud or hybrid cloud infrastructures.

AI excels at automation, optimizing tasks such as deployment, configuration, and system monitoring, significantly improving operational efficiency. Agencies benefit from best-in-class capabilities across multiple CSPs, each offering distinct strengths. Moreover, AI deployment becomes more cost-effective when models are situated closer to the data processing location, making the flexibility to choose the optimal CSP for each use case essential.

As agencies work to implement AI in the cloud, many capabilities still require support from data scientists and ML engineers. But as technology progresses, Reyes predicts these processes will become more intuitive, even for staff without advanced ModelOps backgrounds.

“We used to have to train humans in how to interact with machines, but we’re now training machines to know how to interact with humans. What’s going to become really important is being very specific in how you ask for things and being a great critical thinker,” Reyes stresses. “I can see a fully integrated environment where AI seamlessly enhances every aspect of the cloud, allowing for more accessible and powerful AI tools for agencies to derive insights.”

Of course, as agencies juggle new cloud capabilities and multiple CSPs, they inevitably create new vulnerabilities that need to be addressed.

“This makes data governance policies more important, necessitating regular audits of those security controls and governance policies,” Reyes emphasizes. “There are many AI tools that can help you do that, too.”

How AI can enhance cloud security

In the increasingly interconnected environment created by cloud computing, cyber teams are tasked with sifting through massive amounts of information in search of vulnerabilities and threats. AI helps in a variety of ways, most of which fall under three categories: risk assessment, threat detection, and security automation.

AI-driven risk assessment

- Dynamic threat analysis: AI continuously monitors and analyzes cloud data traffic, adapting its risk models in real-time to identify emerging vulnerabilities and threats.
- Predictive risk insights: Leveraging historical and real-time data, AI provides predictive analytics to forecast potential security breaches, enabling proactive mitigation strategies.

> **"We used to have to train humans in how to interact with machines, but we're now training machines to know how to interact with humans. What's going to become really important is being very specific in how you ask for things and being a great critical thinker."**
>
> **FRANK REYES, MANAGING DIRECTOR OF SOFTWARE AND INFRASTRUCTURE CAPABILITIES, MAXIMUS**

Enhanced threat detection

- Behavioral anomaly detection: Analyzes typical user and system behaviors, flagging deviations as potential threats, ensuring rapid identification of unauthorized or malicious activities.
- Adaptive response mechanisms: Through machine learning, AI systems continually refine and adapt their security protocols based on new threats, ensuring evolving protection against sophisticated attacks.

AI-powered security automation

- Routine security tasks: Utilizing machine learning to streamline and bolster repetitive security tasks, enhancing threat response times and reducing manual oversight.
- Autonomous self-repair: Leveraging AI-driven algorithms to proactively identify, diagnose, and rectify system faults or vulnerabilities without human intervention, enhancing system uptime and resilience.

Cyber attackers often operate like would-be thieves walking down a street, trying every car door until they find one unlocked. Similarly, threat actors will look for existing vulnerabilities to exploit rather than creating a new entry point.

"An attack surface management tool will look for those 'door entryways' and say, 'This is open, you may want to consider patching it or turning that feature off,'" Carver explains.

It's all part of a general push to be more proactive than reactive. By using tools to actively monitor and look for vulnerabilities, agencies can improve their risk posture and reduce time and money spent on reacting to breaches. Just as modern, automated security systems now alert homeowners to unlocked doors or disabled alarms, automated cyber tools highlight security gaps.

"These tools are proactively covering my security boundary and defending that for me," Carver explains. "And it's telling me in real-time what corrective measures I should take to prevent that vulnerability."

The key to creating reliable, proactive security structures is investing in the continuous training and monitoring of AI models and their underlying data. This will ensure the models perform how they're supposed to and can help discern between malice and mistakes.

"Is it bad data, natural drift or management-related, or is it nefarious?" Reyes says. "That takes its own set of understanding, of being able to know when something is deviating from wanted behaviors because it's just broken versus being attacked."

CHAPTER THREE: AI AND DATA

Data is the foundation of policymaking, and efficient, accurate data management is essential to leveraging data as a strategic asset. By automating tasks, from data collection and processing to data cleansing and labeling, AI helps to improve the overall quality of data management.

“You’ve always heard the adage ‘garbage in, garbage out,’ and that holds true today,” says Neil Kronimus, managing director of technology strategy and solutions at Maximus. “But AI can be used to identify outliers or anomalies and enrich the features in the toolsets to make sure data quality is better. It’s all about being able to make better-informed decisions through AI.”

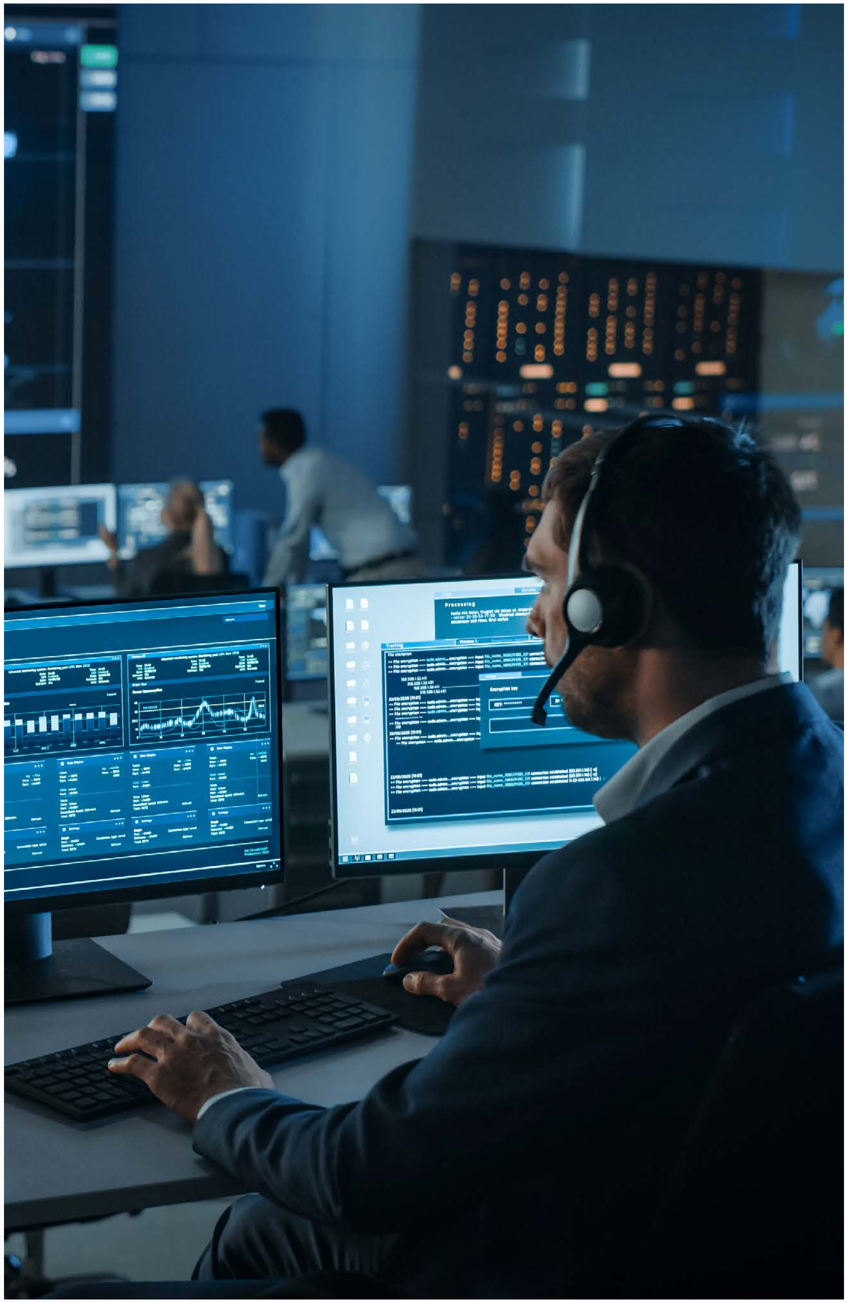
Simplifying government data sharing

The ability to easily exchange data between departments and agencies has been a hurdle for government organizations looking to maximize data-informed decision-making. Add in government-specific regulations and compliance requirements and information sharing becomes even more complicated. Laws and regulations are products of their time, and technology progresses faster than policymaking.

“It makes adoption a little more challenging because sometimes it’s like putting a square peg in a round hole,” Kronimus notes. “It’s about finding the right use cases and workloads that still follow compliance rules, but also help agencies move forward until those rules and regulations are updated.”

From a technical perspective, AI can standardize data formats between unstructured and structured data and simplify the extract, transform, load (ETL) process – a necessity for sharing and combining data sets. In fact, zero-ETL capabilities show promise in eliminating the ETL burden altogether.

“Zero-ETL can bring the data together and let the system behind the scenes transform the data that it’s extracting, so the user doesn’t have to,” explains Kronimus. “That’s where AI comes in, because without AI, the whole idea of zero-ETL would be extremely challenging.”



> **“From predictive analytics and forecasting models, to anomalies, outliers and potential risks, this is where AI can really help. An analyst today is looking at large sets of data for patterns and it’s a repetitive task. Let AI take the lead on that.”**
>
> **NEIL KRONIMUS, MANAGING DIRECTOR OF TECHNOLOGY STRATEGY AND SOLUTIONS, MAXIMUS**

Federal agencies tend to have unique ways of managing information, and even their own data lingo, which can make sharing complicated, Kronimus adds. Natural language processing tools can help harmonize data sets between agencies.

From an analytical perspective, AI can discover hidden patterns or relationships in data that a human might miss, simply due to the sheer amount of information that needs to be studied.

“From predictive analytics and forecasting models, to anomalies, outliers, and potential risks, this is where AI can really help,” Kronimus notes.“ An analyst today is looking at large sets of data for patterns and it’s a repetitive task. Let AI take the lead on that with the human proving the findings.”

Getting leadership onboard

When leveraging AI in data management, key concerns that government leaders express can be simplified to: Where is the data coming from and where is it going? The former is about traceability.

“If we’re not pulling data in from good sources that are reliable, we’re not going to get reliable data out,” Kronimus explains. This can result in decisions that are based on incorrect information, or potentially even biased, depending on the source.

The latter question – where is it going? – is about privacy and security. Government agencies handle sensitive information about everything from government operations, critical infrastructure, and national security to individuals’ personal data. This naturally makes leadership skeptical about new tools and technologies that touch data.

“Going back to the early cloud days, the number one concern was, ‘I don’t want to go to the cloud because of security,’” Kronimus says. “Now with AI, it’s the same thing, people are worried about the security and privacy of their data. It’s going to take some time to gain confidence.”

This is where industry partners like Maximus can offer support, helping agencies ease into AI-enhanced data management by starting with lower-stakes, non-production data, then moving into back-office production workloads, and finally applying tried and true AI tools to mission workloads. Meanwhile, partners can also ensure the right monitoring, evaluation, and audit practices are in place, “so the customer can feel confident that whatever is coming out of the AI model, what they’ve asked for, they can trust it,” Kronimus adds.

CHAPTER FOUR: THE FUTURE OF AI IN GOVERNMENT

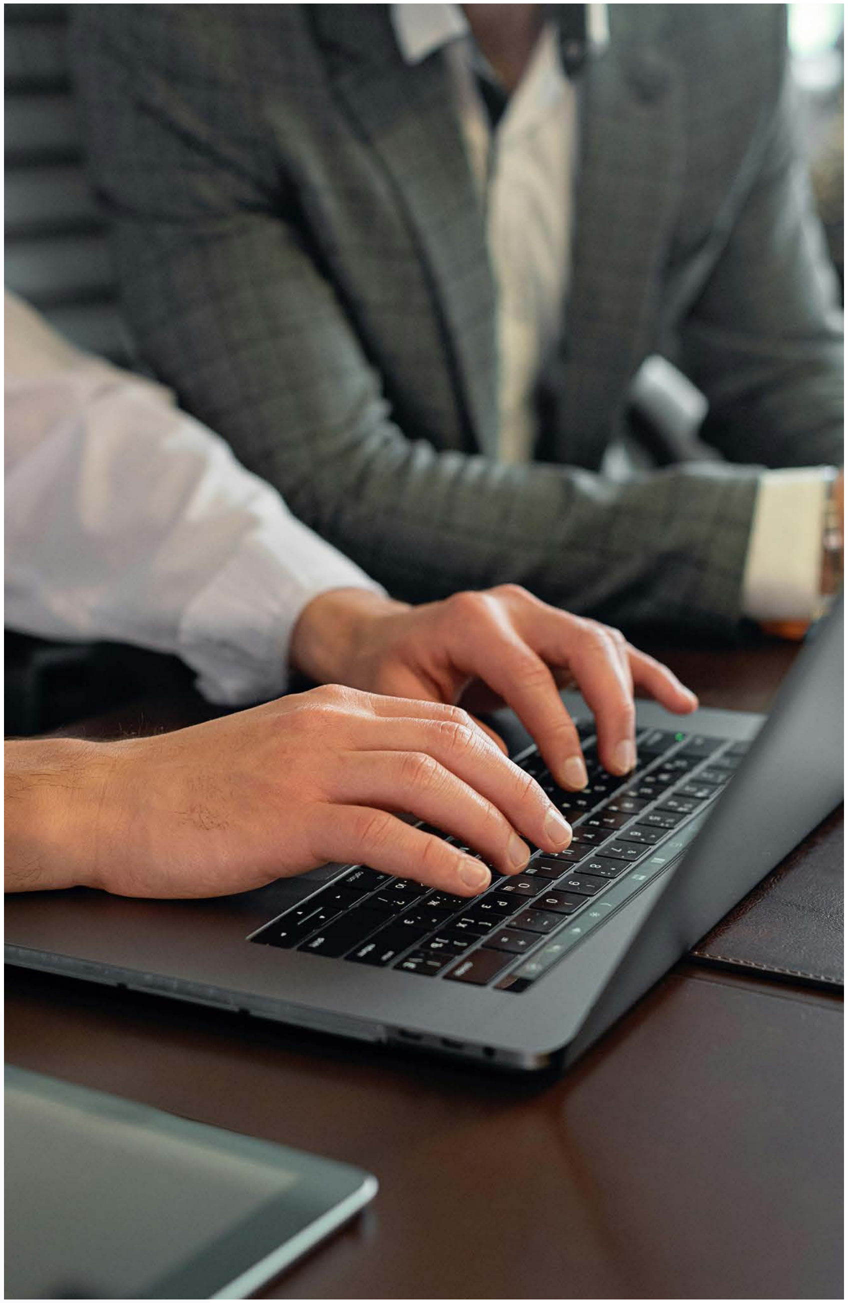
A major step toward integrating AI in government was the release of the "Executive Order on the Safe, Secure and Trustworthy Development and Use of Artificial Intelligence" and the subsequent releases that are continuing from OMB, NIST, International Forums, and at the state level. These actions mark a historic, widespread acknowledgement that AI will be a central part of future government operations. Among the EO's specific action steps:

- Agencies are "discouraged" from enacting broad bans on generative AI products in favor of limiting access based on specific risk assessments and guidelines and, "with appropriate safeguards in place, [agencies should] provide their personnel and programs with access to secure and reliable generative AI capabilities, at least for the purposes of experimentation and routine tasks that carry a low risk of impacting Americans' rights."
- The Executive Office of the President is establishing a White House Artificial Intelligence Council "to ensure the effective formulation, development, communication, industry engagement related to, and timely implementation of AI-related policies, including policies set forth in this order."

"Recent regulatory guidance urging agencies to leverage their established authorities for the responsible use of AI has shifted the conversation from 'if' we will use AI to 'how' we will use it,'" Featheringham states. "This has resulted in a paradigm shift, emphasizing the importance of ethical implementation and strategic integration of AI technologies to enhance public services and operational efficiency."

With this paradigm shift comes the need for shifts in governance. Digital strategy and AI strategy will no longer be separate entities. As with previous technological advancements that became mainstream, such as the internet and cloud, AI is poised to become interwoven into agencies' overall governance structures.

"Years ago, people said, 'Wait, I'm not in the internet business.' Then the internet investment and development capabilities expanded to the point that it's part of everything," Holder says. "In the near future,



artificial intelligence services are going to be part of everything you do in terms of developing digital products."

Even as the nation's leaders work toward fully integrating AI, and the democratization of innovations that it brings, the human element remains central to ensuring ethical use and accountability.

"You need different human perspectives because it really is about human intelligence and improving people's experiences," Holder says. "Ultimately, technology is the enabler, and we're getting to the point where these technologies can do things that humans by themselves cannot do. That's where some of the opportunity and some of the fear comes from, but everyone has a stake in the responsible and ethical use of AI."

MAXIMUS EXPERTS LOOK TO THE FUTURE

Kathleen Featheringham
Vice President of AI and Machine Learning, Maximus

"When email and the internet emerged, they fundamentally changed how work is done, impacting everyone. These have been referred to as general-purpose technologies. AI is considered one of the general-purpose technologies of our time. Historically, there tended to be one major general-purpose technology at a time. Now, we've entered an era where multiple such technologies – like digital twins, 3D printing, and quantum computing – are simultaneously transforming various fields. AI stands at the intersection of all these technologies, amplifying their impact. However, for AI to be effective, people need to understand and know how to use it. It can't just be hidden in the background."

Raymond Holder
Managing Director of Digital Growth, Maximus

"I often ask people to think about the last time they didn't have a piece of digital technology within arm's reach. At the office. At home. Even in the shower! It is everywhere and has become integral to how we get things done in nearly every aspect of our lives. I believe we'll see a similar proliferation of AI in these digital tools, with waves of AI and machine learning enhancing the development, testing, evaluation, and efficacy of these tools. Soon, it will be hard to find applications or user experiences that aren't being improved by AI services, including those we haven't even imagined yet."

Kynan Carver
Managing Director of Cybersecurity, Maximus

"You can start using generative AI and similar technology to query in more common terms. For example, traditional data querying often requires a complex methodology and specific technical knowledge. By allowing generative AI to develop that search script for you, it significantly speeds up response times. Instead of figuring out how to modify your search script to include specific variables, you can simply state your needs in plain language. This approach enhances our ability to identify and stop malicious activities. Ultimately, that's what we're all trying to do. And I think AI is going to get us closer to that point."

Frank Reyes
Managing Director of Software and Infrastructure Capabilities, Maximus

"We're going to get better at writing more secure, more compliant, better quality code, because the easy stuff – like when you have to write another 'for loop,' or classification, or a vectorization, or an array – machines are really good at doing that coding, so our developers are going to be focusing on the business logic. We're probably going to see a lot more of our developers focusing on creative solutions to business problems. I think we're going to see a lot more of our code being automatically generated for that low-level stuff, and our developers focusing on the higher-level, far more complex types of software capabilities."

Neil Kronimus
Managing Director, Technology Strategy and Solutions, Maximus

"We must make sure we're using AI for what it's meant for, and not what it shouldn't be used for. It's not about displacing people, it's about helping them do their jobs better. There will be new opportunities for people to re-train and relearn new things as AI evolves. We're trying to get to Mars by 2030. That's NASA's goal. Think about how AI can help, not only now in the planning, but also when the crew's heading to Mars. There might be a lack of oxygen, they might have to go into a stasis or something. AI can help guide, perform course corrections because of anomalies in space that we don't even know exist. The promise of AI is tremendous, and I see AI becoming increasingly ingrained in everything we do."