

# BUILDING BLOCKS of Federal AI

## INSIDE:

Responsible AI Development .....	3
Infographic: Checklist for AI .....	6
The Key Role of User-Centered Design in AI .....	11

SPONSORED BY

**maximus**

# From the editor's desk



Amy Kluber, Editor-in-Chief



## The Promise of AI

**A**rtificial intelligence (AI) presents potential breakthroughs for government agencies not seen since the internet was first introduced. In fact, the White House recently released an AI Executive Order that President Biden called “the most significant action, any government anywhere in the world has ever taken on AI safety, security and trust.” Silicon Valley investors are sprinting from one AI startup to the next in hopes of discovering the next Google.

Technology leaders in government see similar impacts over the horizon and are making plans to onboard the tools IT leaders need to leverage the full capabilities that AI and machine learning (ML) can

provide. In preparation, federal leaders are making bigger investments in infrastructure and secure data systems.

Those same leaders are hard at work trying to identify the governance models to provide guidance to industry and academia as fears grow over the ethics behind some of AI’s capabilities and what it could yield. Leaders across the federal government, including Federal CIO Clare Martorana, have the challenge to both prepare their organizations for the internal impacts of AI, but also establish the guardrails needed for external organizations to safely develop this technology. ✨



# Table of Contents

INSIGHTS

## **The Key Principles Behind Responsible AI Development**

Responsible AI development relies on human-centered design and understanding the parameters behind new technologies in the field.

INFOGRAPHIC

## **Elements for Responsible and Operational AI**

9 considerations federal agencies can leverage in their AI plans.

PARTNER INTERVIEW

## **Prioritizing Emerging Technology for Government Missions and Outcomes**

AI can help agencies advance their goals, but balancing risk and reward will be imperative to success.

**Kathleen Featheringham, Vice President, Federal AI & Machine Learning, Maximus**

INSIGHTS

## **User-Centered Design is Key to Putting AI into Practice**

With generative AI growing, organizations are targeting user-centered design to deliver effective solutions at scale.



## The Key Principles Behind Responsible AI Development

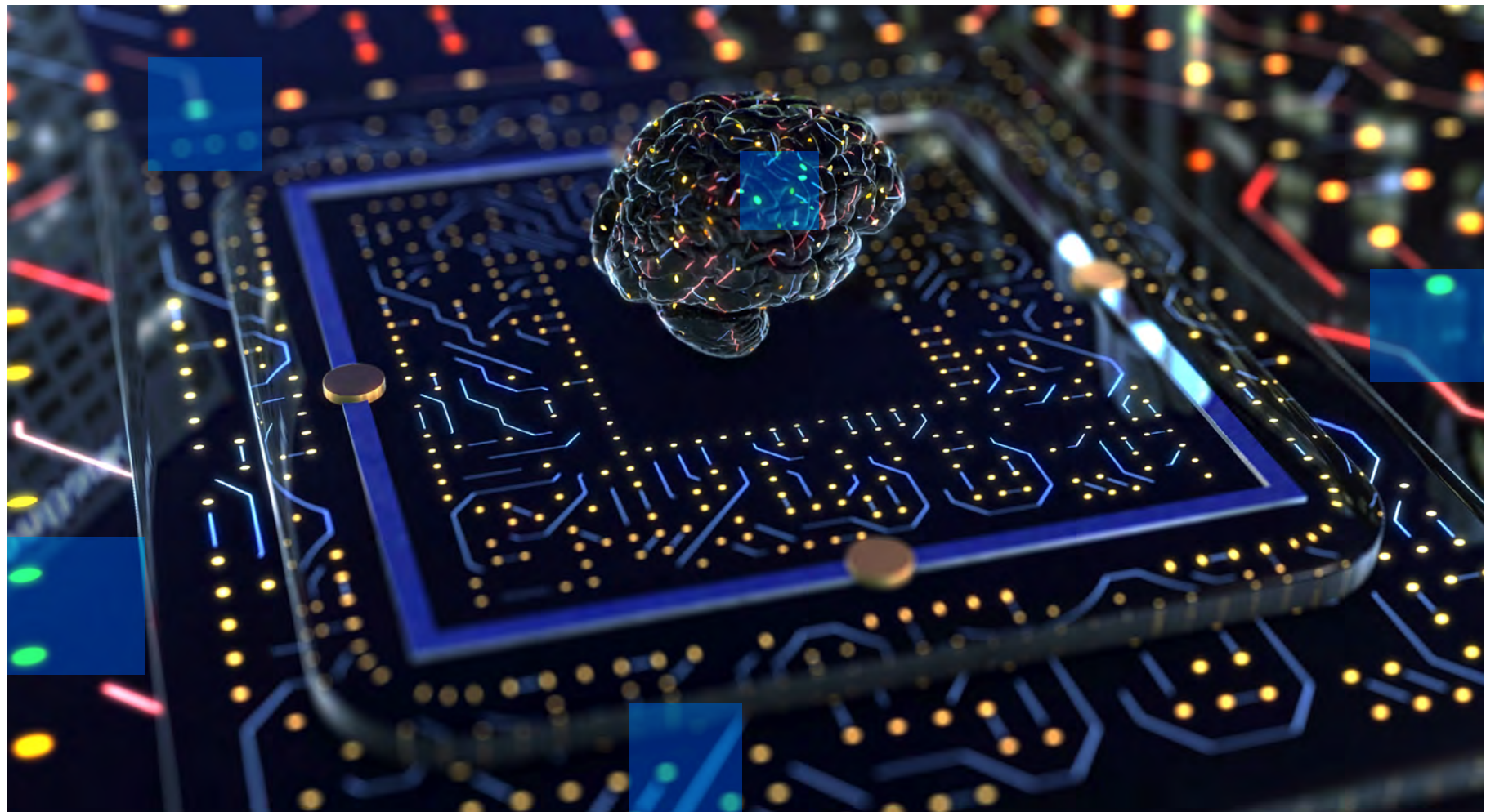
Responsible AI development relies on human-centered design and understanding the parameters behind new technologies in the field.

With the exponential growth of artificial intelligence (AI), federal and industry leaders are creating new governance models to guide the responsible development and use of these technologies.

In 2022, the White House released its [AI Bill of Rights](#) aimed at creating guardrails for AI development and ensuring its responsible use. Major federal agencies helped create the guideline, which includes an outline on safe and effective systems, data privacy, notice and explanation, and alternative options.

“Automated technologies are driving remarkable innovations and shaping important decisions that impact people’s rights, opportunities and access. The Blueprint for an AI Bill of Rights is for everyone who interacts daily with these powerful technologies — and every person whose life has been altered by unaccountable algorithms,” former White House Office of Science and Technology Policy Deputy Director Alondra Nelson told GovCIO Media & Research.

The AI Bill of Rights builds off the foundation of the December 2020 [Trustworthy AI Executive Order](#) that outlined nine distinct principles to ensure agencies “design, develop, acquire and use AI in a manner that fosters public



trust and confidence while protecting privacy.”

With the massive growth of AI technologies over the past six months alone, government is turning to partnerships to drive more innovation and development in AI.

Maximus is taking a human-centered approach to AI development and focusing on key areas, including inclusivity, accuracy, privacy and security. (ctd.)

**Working with leading AI and cybersecurity technology integrators, agencies can balance risk with reward and strengthen commitments to protecting data while improving the overall citizen experience.**

“No data or AI is inherently bad. It’s more about contextualizing what its intended uses are and what goals it is being deployed to address,” Kathleen Featheringham, Vice President of AI and machine learning at Maximus, told GovCIO Media & Research. “For inclusivity and accuracy, let’s say you use a data set from the 1950s, that doesn’t really represent the population today — that wouldn’t be a responsible use.”

By taking a human-centered design approach, Maximus is using key principles behind data use to provide a greater understanding of AI insights and workflows.

### **Understand the datasets being used to train AI models**

AI operates differently than software, offering both deterministic and probabilistic results, whereas software only provides deterministic results. Because of this, it’s essential for AI practitioners to understand how probabilistic results are being obtained.

“If you do not understand where the AI model got its data, it would be an assumption that the outcome was based on a reliable data set,” Featheringham said. “Having visibility into the data that AI algorithms are being trained on is really important because this is your basis for decision-making. If the data used is outdated, inaccurate, or incomplete, that’s going to have an undesirable impact on your ability to make insightful decisions.”

In regard to understanding the data being fed into the AI model, Featheringham is focused on understanding the pedigree of the data, the audit trail and where to incorporate it to create a data lineage.

“When you’re going to put these things together to tune it, bias could have been built into the dataset, for example,” Featheringham said. “You are never going to eliminate bias, but it’s important to understand the bias and be aware of it, so you are making decisions based off those parameters.”

(ctd.)





## **Establish AI governance frameworks**

Because of these shifting aspects of AI, organizations must continuously evaluate governance models. Featheringham said with AI, “it’s about understanding the mindset difference, that it’s always going to be potentially shifting.”

“The thing about the governance is: Who should be involved in it, and what role do they play? Where should they be involved in terms of that decision-making? There’s no one right answer,” Featheringham added. “Agencies may be able to leverage existing governance frameworks, building in new policies and procedures to address AI tools and how they impact associated workflows.”

## **Address change management**

Looking ahead, Featheringham is emphasizing “cohesive collaboration” with government and industry partners to better understand and democratize data, as well as improve workforce readiness.

“Change management is critical. It’s important to ensure continual education and recognize the speed of change that is required to be successful for workforce readiness in the use of AI,” Featheringham said. 🌸



## 9 Elements for Responsible and Operational AI

### Responsible

- ✓ Understand and mitigate bias in data sources
- ✓ Create AI audits to ensure compliance and traceability
- ✓ Maintain appropriate compliance measures
- ✓ Utilize human-centered design from the start
- ✓ Evaluate tools for near-term vs. future use based on their relative maturity level

### Operational

- ✓ Determine the desired mission outcome
- ✓ Understand parameters that led to the decision
- ✓ Incorporate into existing workflows to increase efficiencies and enable workforce to allocate time to other tasks
- ✓ Create change management plans and adapt governance models



PARTNER INTERVIEW

# maximus

## Prioritizing Emerging Technology for Government Missions and Outcomes

AI can help agencies advance their goals, but balancing risk and reward will be imperative to success

 **How is the federal conversation around artificial intelligence (AI), machine learning (ML) and automation evolving?**

**Featheringham** The proliferation of AI-enabled systems and devices, as well as new generative AI tools, has given rise to a rapidly evolving conversation among federal agencies and their technology consulting partners.

In recent months, the White House took action to promote responsible AI innovation across government programs. Public and private organizations, government agencies and citizens want to ensure that AI is being developed and implemented responsibly as the field continues to advance.

At Maximus, we emphasize responsible use by defining what we want to achieve while focusing on outcomes to support our customers' missions. We want to understand who will be interacting with



**Kathleen Featheringham,**  
Vice President, Federal AI & Machine Learning, Maximus



**“The focus should be on how AI can be used responsibly to drive mission outcomes and provide the best citizen experience – and this requires understanding the technology’s opportunities and limitations in order to maximize value.”**

**— Kathleen Featheringham,  
Vice President, Federal AI & Machine  
Learning, Maximus**

the AI and how, what data is being used to train the tool and how precise its output needs to be based on the specific use case. These considerations factor into the evolving conversation with agencies, experts, industry and others around issues critical to ensuring responsible AI innovation.

 **What should agencies prioritize over the next year to leverage AI to support mission outcomes?**

**Featheringham** The maturity level of different AI tools is a critical factor in determining how they can be used responsibly in the short term versus the future.

For instance, when our clients are looking to improve citizen self-service capabilities, we leverage an Intelligent Virtual Assistant (IVA) that uses speech recognition, human-assisted AI and natural language processing to enable automated, conversational interactions. For example, as part of our work with the Centers for Disease Control and Prevention (CDC) supporting CDC-INFO – a critical component of CDC’s emergency response communication infrastructure – we use AI-based sentiment analysis and topic modeling to identify trends and improve the customer experience.

These relatively mature AI tools can accelerate value to federal agencies and the citizens they serve. This simplifies the interaction and routes it to the most appropriate resources quickly and efficiently. This also allows human personnel to focus time on complex tasks and problems.

 **What are the risks and opportunities with AI, ML and automation that agencies will need to mitigate and respond to?**

**Featheringham** As AI evolves rapidly, the focus should be on responsible use to drive mission outcomes and to provide the best citizen experience. This requires understanding the technology’s opportunities and



limitations to maximize value. These include implications for data quality, availability and security.

Currently, there is concern over data quality in generative AI technologies, given the amount of inaccurate data on which these tools train. While this concern is valid, the data-quality risk will decrease over time as private and secure data sets improve the output accuracy. In the near term, agencies can decrease risk by educating staff on how these tools could or should be used, including implementing processes to validate the tools' output and correct it as needed.

When it comes to data availability, new AI technologies may help increase it. For instance, generative AI can create synthetic data sets that, in turn, can be used to train new AI and ML models. This increases the amount of data generated and can improve data access through automation, boosting user experience.

AI and ML might also help address data security with the capability to check large amounts of code for vulnerabilities. An important caveat: In the hands of bad actors, these capabilities can present risks of generating inaccurate data sets or malicious code, thereby increasing vulnerabilities. Working with leading AI and cybersecurity technology integrators, agencies can balance risk with reward and strengthen commitments to protecting data while improving the overall citizen experience. 🌟





# Maximizing the benefits of AI for government agencies

LEARN MORE

maximus



# User-Centered Design is Key to Putting AI into Practice

With generative AI growing, organizations are addressing user-centered design to deliver effective solutions at scale.

Generative AI is booming in popularity, and now tech leaders are leveraging user-centered design principles to deliver data-driven decisions at scale to meet mission needs.

Federal CIO Clare Martorana encourages agencies to explore AI use cases for cutting down manual workloads while driving higher value.

“There’s a lot of work going on, both on the rules and regulations, but also on the way that the government does need to lean into this to make sure our workforce is best equipped and best enabled to meet the moment,” she said. “It’s about communication and us being open, transparent and willing to share information, and not hoard the information to be able to bring us all along on the journey. Because the technology is not going to slow down. We have to speed up.”

Federal agencies are looking to innovate at the speed of industry, while also developing guidance and frameworks to outline the responsible use of these emerging technologies. Maximus describes this shift as becoming more



“user-focused.”  
“AI is going to be an incredible set of tools that will take us almost into a new century of technology,” Joe Jeter, Senior Vice President of Federal Technology at Maximus, told GovCIO Media & Research. “Agencies need to look at the current problem set and say, ‘How can AI improve outcomes to missions, the speed in which AI can execute a mission, and evolve a set of requirements that create new missions?’ I think we’re at a tipping point where

the tools are now becoming user-focused as opposed to developer-focused.”

Jeter is focusing on getting the right data to the right users at the right time to bolster the human-centered approach to AI. While the vision is clear, agencies and organizations face a few common hurdles, including compliance.

“Where does data come from? Can we use that data? Then, the third thing we have to do is understand the impact on infrastructure. Then, cybersecurity. How does that all work together?” he said.

To overcome those barriers, the first step is to determine the outcome, (ctd.)





**Clare  
Martorana**  
Federal CIO

then focus on the end goal through a “compliance lens,” Jeter said. This methodology fits into the human-centered design approach.

“I’m looking for the outcome and then the use case as the foundation of how we build a solution. Once we have that outcome and use case in mind, we come back and say, what are the sources of data? What are the rules of compliance? What are the access requirements? What are the data extraction tools? Then, what’s the roadmap? What are the impacts?” Jeter said.

Then, Jeter said focusing on auditing the data creates traceability into the impacts of the data and outcomes of the AI tools.

“Those AI audits are looking at the use of this technology, the nature of compliance and the traceability of data — who used it?” Jeter said. “We’ll see a new generation of assessment tools, just like what we saw with cyber.”

“There’s a set of fundamentals we’re going to expect out of the infrastructure, so now when we’re thinking about continuous improvement, it’s how do I evolve my use case for better outcomes and impacts?” Jeter said.

Looking ahead, Jeter said the explosion of generative AI has created new user expectations for instantaneous results, which require a near-immediate response time, more computing at the edge and scalability.

“You’re going to see new architectures to deliver the answer, and the use case is going to drive architectures,” Jeter said. “At the architectural level, we’re saying now we have to solve for 1,000 questions, not just one question. Now, we have to think about it from a sizing standpoint. How do we size for an expanded user community that knows how to use technology? At Maximus, we make AI operational to create scalable operations for the government.” ❁

**“There’s a lot of work going on, both on the rules and regulations, but also on the way that the government does need to lean into this to make sure our workforce is best equipped and best enabled to meet the moment.”**

**— Clare Martorana, Federal CIO**