MeriTalk

"ALL IN" WITH AI:

HOW TO SPEED GOVERNMENT ADOPTION

AFFILIATES:

elastic

FUTURE TECH

DELL Technologies
TITANIUM PARTNER

leidos

ORACLE
Cloud

stackArmor

FORWARD:

MeriTalk recently convened an elite group of government and security experts to consider a critical question facing Federal policymakers: How to accelerate safe and secure artificial intelligence (AI) deployment in government. **The Accelerate AI Forum dove deeply into AI operationalization, acquisition, security, and governance through panel discussions with the following speakers:**

Dorothy Aronson, Chief Data Officer and Chief Artificial Intelligence Official, National Science Foundation

Teresa Carlson, Advisor and Investor, General Catalyst

Dan Chaney, Vice President, Enterprise AI and Data Science Solutions, Future Tech

James Donlon, Director, Solution Engineering, Oracle

Dave Erickson, Public Sector Distinguished Architect, Elastic

J. Matt Gilkeson, Division Director, Innovation Task Force, Transportation Security Administration

Ron Keesing, Senior Vice President, Technology Integration, Leidos

Suzette Kent, former Federal Chief Information Officer, Office of Management and Budget

David McKeown, Senior Information Security Officer and Deputy Chief Information Officer, Cybersecurity, Department of Defense

Gaurav Pal, Chief Executive Officer and Founder, stackArmor

Maria Roat, former Deputy Federal Chief Information Officer, Office of Management and Budget

Dr. Anna Rubinstein, Chief, Responsible Artificial Intelligence, National Geospatial-Intelligence Agency

Vinay Singh, Chief Financial Officer and Chief Artificial Intelligence Officer, Department of Housing and Urban Development

Martin Stanley, Strategic Technology Branch Chief, Cybersecurity and Infrastructure Security Agency

Kevin Walsh, Director, Information Technology and Cybersecurity, Government Accountability Office

Federal agencies are ramping up their AI use, yet challenges and complexities abound. While AI technologies are advancing at breakneck speed, Federal institutions and processes are not designed to move as quickly.

The AI executive order (EO) and implementation guidance are introducing numerous requirements for agencies, which must integrate AI systems into existing security protocols – while rapidly deploying the technologies and respecting the privacy of citizens. Integrating these new requirements present a series of emerging procurement and implementation barriers.

Even amid the obstacles, a consensus is emerging among those entrusted with running, securing, and working with our government: With the EO's galvanizing effect and competition with China and other U.S. adversaries, now is not the time to slow down. As Vinay Singh, the Department of Housing and Urban Development's chief financial and artificial intelligence officer said at MeriTalk's Accelerate AI Forum, AI means "all in."

Government and industry experts explored AI operationalization, acquisition, security, and governance at the forum and offered a series of tangible suggestions for how to expedite getting AI tools into the hands of Federal leaders who need them. Their recommendations are outlined below.

OPERATIONALIZING AI

The Federal government has been using AI in some form for about 40 years, but for most of that time, the technology remained in the exclusive realm of scientists and researchers. Today, owing to the advancement of computing power, data maturation, and large language models that can be easily applied, AI is seemingly everywhere.

AI's revolutionary potential could be transformational for many government purposes, and Federal agencies have been focusing on how to more quickly – and safely – operationalize AI technologies to support a range of missions.

In many ways, the question of deploying AI in government has been answered, because AI is already here. A recent U.S. Government Accountability Office (GAO) report found that 20 Federal agencies reported 1,200 current or planned AI use cases. The recent AI Executive Order has invigorated the discussion around AI within agencies even more.

While there is much attention to applying AI to operational mission areas, the procurement and implementation barriers and a lack of security and governance controls have prevented Federal officials from moving rapidly to fully harness AI's immense power.

To operationalize AI at a higher level, forum participants recommended these tangible actions:

Train the workforce.

The Department of Homeland Security, for example, began training employees on generative AI tools in recent months. "Everyone is going to have access to these tools whether we bring them in house or not," said Dorothy Aronson, chief data officer and chief AI official at the National Science Foundation. "So if you don't train people, they'll misuse it. I think we have to run as fast as we can to get this done."

Test AI systems rigorously.

At the Transportation Security Administration, officials regularly test security detection algorithms to ensure that they meet architectural standards and don't overly trigger false security alarms. "I love the testing conversation," said James Donlon, director of solution engineering at Oracle. "There is so much smart and effective testing to be done with generative AI in particular, and I would encourage my Federal counterparts to start asking questions of large language models when you have time. You might be surprised at the results"

Move fast but start small.

One forum participant recommended: "Do the low-hanging fruit AI pilot and show employees how it doesn't take away their jobs, but it does help them do their jobs."

Learn from the private sector.

Speakers unanimously urged Federal IT leaders to work with industry to deploy AI technologies more efficiently. This area of discussion also included new attention to data and data sources. One factor that will help promote public-private partnerships is that unlike some other previous technology trends, "industry and government are much more aligned in the adoptive curve for AI," said Suzette Kent, former Federal CIO for the Office of Management and Budget (OMB).

ACQUIRING AI

Operationalizing AI means acquiring the various tools that make up an AI system – and working within a procurement system that experts say is piecemeal at best. In fact, GAO recently concluded that the U.S. still lacks government-wide guidance "on how agencies should acquire and use AI."

Experts say AI acquisition is perhaps the most complicated part of an overall AI ecosystem that requires weaving together the priorities of the new EO with various existing protocols for deploying technology inside the Federal government.

Much of the challenge, one industry expert said, stems from the warp-speed advance of AI technologies. "When you look at this from an acquisition perspective, you're jumping into a river," he said. "By the time you figure out what the solution is, the software changes – it's ever-changing."

To adapt to – and overcome – the existing AI acquisition landscape, experts who spoke at the forum offered these insights:

Experiment.

The National Science Foundation, for example, recently surveyed employees for ideas on how to best adopt AI into their missions. The agency is now embarking on a pilot program stemming from one of those ideas, seeking to learn more about procurement and other implementation barriers.

Don't design in a vacuum.

Refrain from purchasing components "ahead of the demand curve" because the state of the art may change before technology can be procured. "Buy based on what you know you need to solve today and your next two or three steps," said Dan Chaney, vice president for enterprise AI and data science at Future Tech. "Working with a partner ecosystem can ensure you buy what you need when you need it. AI is complicated, and working with the right partners is key."

Remember that AI is not one-size-fits-all.

Experts emphasized that purchasers should evaluate multiple hardware, software, and other solutions – don't "just buy a block of AI" – and figure out next steps after they have operationalized AI and evaluated the outcome.

Coordination is key.

To succeed with AI, collaboration and coordination among acquisition, cybersecurity, privacy, compliance, and other agency stakeholders, as well as industry partners, is essential – from the beginning of every project.

ALIGNING AI WITH SECURITY

The General Services Administration (GSA) recently unveiled a draft framework for how its Federal Risk and Authorization Management Program (FedRAMP) will prioritize certain cloud offerings that include generative AI technologies.

Mandated by the recent AI EO, GSA's offering was the latest in a series of new security frameworks prompted by concerns that the technology can create potential attack surfaces, even as it can also enhance cybersecurity by fending off phishing and malware attacks.

Among the frameworks, perhaps most prominent is the National Institute of Standards and Technology's (NIST) AI Risk Management Framework. The NIST framework is a solid example of guidance needed to protect AI systems and data, experts say.

> The framework "brings people to the table to talk about what are the benefits, opportunities, and potential harm of using AI."
>
> **Martin Stanley**
> Strategic Technology Branch Chief
> Cybersecurity and Infrastructure Security Agency (CISA)

More recently, CISA collaborated with more than 20 domestic and international cybersecurity organizations – including the Federal Bureau of Investigation and the National Security Agency – to release Guidelines for Secure AI System Development.

While "AI systems have the potential to bring many benefits to society," the guidelines say, "AI systems are subject to novel security vulnerabilities that need to be considered alongside standard cybersecurity threats."

Dave Erickson, public sector distinguished architect at Elastic, emphasized AI's capacity to help improve security. The "disruptive, gold rush-type of challenges presented by AI are very exciting," he said. "The key is to take our best cyber protectors and give them that force multiplier, which is AI."

To implement AI as securely as possible, experts offered these suggestions:

Learn from cloud. While FedRAMP was established in 2011 to empower agencies to securely use cloud technologies, the program was not codified as "the authoritative standardized approach to security assessment and authorization" for cloud computing projects until 2022. "It took us over 10 years to get from ideation to law. That's crazy," said Teresa Carlson, a former top executive at Amazon and Microsoft. "AI is going to move much faster – there is no doubt … agencies are going to want to adopt, they're going to want to use it." Another lesson from the cloud journey: To capture the highest level of benefit, remember to give strategic consideration to all AI components–software, data, infrastructure, and people.

Apply zero trust principles. Although AI's arrival in the Federal space as agencies work to implement mandated zero trust security measures has caused concerns about potential complications, experts say AI security and zero trust actually complement each other. One government official called for "employing some of the zero trust concepts we've been working on to make sure that once we've already tested an algorithm, it seems to work and it's delivering results as we continue to monitor."

Partner with industry. "We're huge partners with industry," one government official said. "We have to bring these use cases to industry. Certainly, we want to leverage our partnerships with industry for cybersecurity."

Participate. Government officials asked for feedback when an agency releases a new AI security protocol. CISA, for example, recently unveiled a request for information on its secure-by-design software practices. The agency is seeking input on additional security considerations necessary to develop secure AI, noting that "AI is software" and should adhere to secure-by-design principles.

AI GOVERNANCE

Overseeing these areas of AI is a governance structure that is still evolving as the technology becomes more prominent in Federal operations.

Throughout the forum, experts described a series of what they called "thou shalts" – outlined in government guidance documents on AI released over the past five years that require increasing Federal action.

The 2019 AI executive order and the 2020 AI in Government Act, for example, required OMB and other agencies to issue memos and other documents aimed at developing policies to regulate AI use in the Federal space.

The recent EO substantially expanded that governing structure, directing 50 Federal entities to take nearly 150 specific actions covering eight broad areas of AI policy.

In late January, the Biden administration released a three-month progress report, which concluded that agencies have been making "substantial progress" in meeting key EO goals.

Federal leaders are making progress, but much work needs to be done to establish a comprehensive structure that truly oversees AI deployments with smart governance, forum participants said.

> "These early steps seem relatively straightforward, and what we're hearing is a great deal of concern about what happens in the future."
>
> **Ron Keesing**
> Senior Vice President for Technology Integration
> Leidos

He said Leidos is developing an AI assessment framework for government customers seeking help in their AI journeys. "We'll get there," Keesing said. "It is still early in the process of AI integration into Federal agencies, and governance structures just need time to catch up."

To help agencies along, experts suggest:

Consider governance throughout deployment planning: Individual agencies should take the lead on AI governance as much as broader governmental bodies. The National Science Foundation, for example, has created a flexible set of processes for deployment, merging its AI governance and AI data functions. The National Geospatial-Intelligence Agency, also seeking to improve its governance structure, will soon release training protocols for AI mobile developers and system users. That follows the agency's earlier studies comparing AI-enabled workflows to legacy system workflows.

Follow chief AI officers' lead. Agencies throughout the government should follow the guidance of the chief AI officers being appointed at Federal agencies, as mandated by OMB in its proposed guidance implementing the recent EO.

Even as AI governance advances in fits and starts, forum participants predicted that Federal officials will develop more effective oversight – and that the power of AI will itself alter the structure of government.

"We are on the cusp of massive, massive change in the way government works," said Kevin Walsh, director of information technology and cybersecurity at GAO. "We're going to be putting in new governance structures. There are a lot of requirements for AI that the government is going to have to address, and we are going to be faced with a decision: Do we create separate silos for AI, which is the easy thing to do? Or do we try to blend it into already existing processes and take advantage of the oversight … and the capabilities that we already have?"

Incorporating AI into existing governance structures will be more difficult, but it will be crucial to ensure the success of the technology going forward, Walsh said. When you make AI "separate and different," he said, people "don't go down that road."

CONCLUSION

If one overriding lesson emerged from MeriTalk's Accelerate AI Forum, it is that AI deployment in the Federal government does indeed need to move faster.

The challenges are great. Chief among them is the complexity of AI systems, which requires multiple components – operationalization, acquisition, security, and governance – to be woven together into a seamless whole that follows existing protocols while creating something new.

Yet optimism abounded that the complexities can be solved – and that AI is destined for a great Federal future. "AI has catapulted to the forefront of the minds not just of technologists, but of people everywhere," said one forum participant, who added this summation of the road ahead for AI deployment in the Federal space: "Let's get going!"

AFFILIATES:

elastic

Future Tech

DELL Technologies
TITANIUM PARTNER

leidos

ORACLE
Cloud

stackArmor