FEDInsider

Scaling Government AI Takes More Than a Successful Pilot

Experts discuss the people, processes and safeguards needed to turn isolated experiments into enterprise-wide, mission-focused capabilities.

Featured Experts:

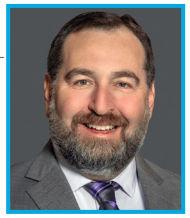
- **Rebecca Cai**
  Chief Data Officer,
  State of Hawaii



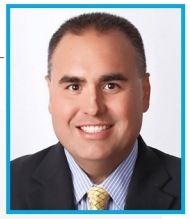
- **Monica McEwen**
  Principal, Deloitte U.S. Government, Public Sector AI & Data Leader



- **Josh Salmanson**
  Vice President, Defensive Cyber & Resilient Network,
  Leidos



- **Steven Boberski**
  Public Sector CTO,
  Genesys



- **Randy Hayes**
  Vice President, Public Sector,
  Vast Data Federal



- **George Painumkal**
  Vice President, Product Management & Product Support, Public Sector,
  Icertis



Successful artificial intelligence pilots do not automatically translate into agencywide results. Scaling requires alignment across leadership, workforce, procurement and mission teams, and that strategy includes moving from use case to capability and from experimentation to operationalization.

During a recent **FedInsider webinar**, government and industry experts discussed the infrastructure, governance and organizational changes needed to turn isolated experiments into enterprise capabilities.

Scaling AI Beyond Isolated Pilots

For the State of Hawaii, deciding whether an AI use case is ready for deployment depends on its scalable business impact, said Rebecca Cai, the state's Chief Data Officer. "There are three things we look for AI use cases. One is governance to manage the risks. Second is the impact to justify the value the AI use case brings. The third one is readiness to assess the efforts involved and the real feasibility of the use case," she said.

Having business process leaders act as AI champions also helps to drive transformation in the processes they own. "At the end of the day, this is not really about technology. It is about trust and impact," Cai said.

Echoing much of Cai's comments, Monica McEwen, Principal for Deloitte U.S. Government Public Sector AI and Data Leader, recommends considering similar factors as agencies scale beyond pilots.

The first is the IT infrastructure. "Do you have scalable infrastructure, and have you considered what that would look like if you rolled out AI at the enterprise level?" McEwen asked. The second is security, especially working to ensure that the AI models are structured so that they can only access the data they are permitted to see.

The third is data readiness. That includes data security and governance, and how the data is cleaned and prepared for upstream use. And the fourth is workforce readiness to ensure people are trained to use AI, and have an understanding of why they are using it and with what intent.

Overcoming Common Implementation Challenges

A pilot can prove that an AI solution provides a useful result, but to scale enterprise-wide, it must also provide repeatable, dependable results, said George Painumkal, Vice President of Product Management and Product Support for Public Sector at Icertis.

"There's multiple variables that come in at enterprise scale: more documents and data sources, more variations in data quality, and more users asking the same questions in many different ways, leading to more opportunities for unsupported or inconsistent answers from AI," Painumkal said.

Larger context can bring in more information, but it also gives the AI model more irrelevant or conflicting information, which can cause hallucinations. For a federal agency dealing with millions of transactions, this isn't sufficient for contracting decisions, compliance determinations, financial actions or policy interpretation. Reliability at that scale requires consistent processes with traceability and identifiable sources, data capture for downstream audits and a human review process.

Cost models are another challenge, according to Randy Hayes, Vice President of Public Sector at Vast Data Federal. AI pilots may seem affordable, but

carahsoft. GENESYS Icertis VAST FEDERAL

from an infrastructure perspective, they don't scale completely linearly. Agencies must model how infrastructure costs change as workloads grow across cloud, on-premises or hybrid environments.

"Not only is there cost in scaling the different AI models, but there's also cost in scaling the auditability of all of the different systems. That's so you can show your work and show exactly how you get the answers, and . . . getting the answers back in a consistent way that you expect," Hayes said.

Scaling AI also comes with risk, so agencies must consider how to protect every action, from the pilot stage to the enterprise, without introducing even more risk, said Josh Salmanson, Vice President of Defensive Cyber and Resilient Network at Leidos.

"We tend to focus our frameworks around scaling the trust and not the tools," he said. This allows users to expand what the AI is trusted to do, a single guardrail at a time, while understanding the consequences.

"Governance scales with the consequences and not the convenience of the problem," Salmanson added. "What we're trying to do is make sure we bound the risk by the autonomy we allow the system to have at any point in time."

McEwen added that scaling AI also amplifies existing data problems. Information scattered across legacy systems and formats needs to be integrated and governed, with clear ownership, quality standards and access controls. "The reality is AI does not eliminate bad data debt, it just exposes and accelerates it," she said.

Agencies must trace where data originated, how it changed and which version informed an AI output, McEwen said. That lineage helps teams explain results and understand their limitations.

Building Sustainable, Enterprise-Wide AI Solutions

Resource reductions and limited workforce bandwidth can stall promising AI efforts, Cai said. Hawaii is addressing that challenge with its AI champions who guide redesign and adoption, while technical teams support tools, data and governance.

Those champions must understand and own the full process, from initial requests through approvals, including bottlenecks and workarounds. They must also have colleagues' trust and remain responsible for improving the process as tools and risks change.

The approach can also help agencies scale. When a champion redesigns a common process, like hiring or procurement, other agencies can adopt it rather than starting from scratch. "The biggest lesson is AI transformation is really business transformation, not IT transformation," Cai said.

Building that trust also requires clear communication with employees and the public, said Steven Boberski, Public Sector CTO at Genesys. "If you don't have a communication plan in place both for the customer and for your employees, you will see resistance and a lack of adoption that will make it incredibly hard to be successful," he said.

Agencies also need continuous monitoring, policies, review processes and human oversight in place before expanding deployment. Boberski said teams must continually assess performance to ensure that customer-facing services can securely provide accurate information. "If you don't have the guardrails in place, you don't have a real program to review your progress," he said.

And because AI forces organizations to stop ignoring their data problems, cybersecurity is critical, Salmanson said, and it starts with identity and data.

Agencies must understand where the tool is pulling data from, the accuracy of the data and whether it'll help improve the context of analysis tools.

"The AI itself is now part of your security boundary and attack surface, and it needs the same segmentation, least privilege and monitoring around any other critical asset," Salmanson said, "and it becomes a more and more critical asset, comparatively because it holds so much mission and enterprise data."

Governance, audit trail capability and human-in-the-loop checkpoints must be built into the AI solution from the start, and scaling AI requires agencies to build governance and workforce adoption alongside the technology. "You don't go from no AI to AI automation on day one. You have to phase in the use cases as governance processes and adoption footprints grow within the agency," said Painumkal.

And as agencies begin to look beyond individual AI pilots, McEwen's final takeaway was to keep enterprise adoption focused on mission outcomes, and from there, it's about scaling trust.

"Enterprise deployments will be successful if they're tied to mission outcomes, supported by the reliable data we talked about, governed appropriately and then really embedded into the workforce and processes," she said. "And last but not least, deployed responsibly."

TO LEARN MORE, VISIT CARAH.IO/CARAHSOFTAI

Hosky Communications Inc.
3811 Massachusetts Avenue, NW
Washington, DC 20016
Contact: **John Hosky**

(202) 237-0300
Info@FedInsider.com
FedInsider.com
Facebook.com/FedInsiderNews
Linkedin.com/company/FedInsider
@FedInsider

Carahsoft
11493 Sunset Hills Road,
Suite 100
Reston, VA 20190

(703) 871-8500
Info@Carahsoft.com
Carahsoft.com
Facebook.com/Carahsoft
Linkedin.com/company/Carahsoft
@Carahsoft

Genesys
1302 El Camino Real
Suite 300, Menlo Park, CA 94025
Contact: **Steven Boberski**

(703) 554-5789
Steven.Boberski@Genesys.com
Carahsoft.com/Genesys
Facebook.com/Genesys
Linkedin.com/in/StevenBoberski

Icertis
14711 NE 29th Place
Suite 225, Bellevue, WA 98007
Contact: **Bri Taylor**

Briana.Taylor@icertis.com
Icertis.com
Facebook.com/Icertis
LinkedIn.com/company/Icertis/home/
@Icertis

Vast
8000 Towers Crescent Drive
Suite 1350, Vienna, VA 22182
Contact: **Drew Goldberg**

(607) 220-7071
Drew.Goldberg@VastFederal.com
VastFederal.com
Linkedin.com/company/Vast-Data-Federal

© 2026 Hosky Communications, Inc. All rights reserved. FedInsider and the FedInsider logo, are trademarks or registered trademarks of Hosky Communications or its subsidiaries or affiliated companies in the United States and other countries. All other marks are the property of their respective owners.