Symantec. by Broadcom | Carbon Black. by Broadcom | carahsoft.

Building a Secure Foundation for Government AI

Government leaders are prioritizing data governance, human oversight and targeted investments to support responsible AI adoption.

Featured Experts:

- **Rudolf Rojas**
  IT Program Manager & Security Lead, USDA

- **Tony Batalla**
  Chief Information Officer, City of Oakland, CA

- **Alejandro Loza**
  Technical Director, Broadcom Enterprise Security Group

As agencies rush to expand their use of artificial intelligence to meet federal mandates, legacy systems and fragmented data can complicate deployment, increasing systemic risk and creating data-leakage vectors. Deploying AI safely requires clear accountability, reliable data and employees who understand their role in protecting it.

During a recent FedInsider webinar, government and industry experts shared how they're adapting existing security frameworks and establishing human oversight to prioritize investments in data governance and training.

Building Guardrails for Federal AI Adoption

For the U.S. Department of Agriculture, AI governance starts with drawing on existing guidance from agencies such as CISA and NIST. The department also builds on more than a decade of zero trust practices, according to IT Program Manager and Security Lead at USDA Rudolf Rojas.

"Zero Trust is kind of the roadmap we use to indicate everything that we do in terms of security, development, application development and governance," Rojas said.

The USDA is consolidating its disparate data into a shared warehouse with standardized data structures and reporting tools, reducing the need to build ad hoc applications to access information. Securing that data within the department's network is central to making it available for AI and robotic process automation.

Securing internal data is also central to the efforts of Oakland, California to manage AI as an enterprise service. The city's CIO and Director of IT Tony Batalla said the challenge is no longer whether AI has value, but how to oversee its use across an organization.

"It is really a question of how do we transition into something more of an enterprise kind of structure and manage AI as an enterprise service?" Batalla said.

For Oakland, the foundation of that work began with data governance; by identifying how to protect the most sensitive and critical data, what information AI tools should not process, determining what data could be shared and establishing a process to review and authorize the tools themselves.

AI Governance Starts with Accountability

Governance starts with accountability, but it can't stop with written policy, said Technical Director at the Broadcom Enterprise Security Group Alejandro Loza. "That is not governance."

The use of AI leaves an organization with more questions to consider, like: What AI is being used? What data is being exposed (by whom and for what purpose)? What controls apply?

In the past, those controls were defined by simply blocking whatever devices were trying to gain access. With AI, control exceeds access because AI can make decisions and access systems itself if proper controls are not in place — and if no one is assigned to that oversight.

Following the Office of Management and Budget Memorandum M-25-21 titled "Accelerating Federal Use of AI through Innovation, Governance, and Public Trust," is a great start, but Loza said for high-impact AI, "you really need additional practices including pre-deployment testing, impact assessment, ongoing monitoring and human oversight."

The USDA is taking a measured approach to AI adoption given its role in supporting critical

food and agricultural infrastructure, Rojas said. The pace and direction of adoption may depend on the department's CIO and CISO leadership at the time, but the department evaluates tools with an emphasis on guardrails and a clear return on investment. The agency also requires stringent human oversight for all AI-based projects.

"We need to retain that human-in-the-loop, so AI does not get ahead of itself, or we get ahead of ourselves using the tools," Rojas said.

Oakland has also made qualified human oversight a critical control for AI use. Batalla said the city's "Meaningful Human Review" requirement calls for someone with relevant subject matter expertise to assess whether an AI-assisted action or tool is appropriate before it is carried out.

Putting AI Frameworks Into Practice

Loza said organizations should adapt and expand existing governance processes for AI rather than create additional bureaucracy that could slow down innovation or push users to unapproved tools.

Zero Trust can continuously verify access and permissions for AI agents, along with the NIST AI Risk Management Framework's guidance to govern, map and manage risk, especially as systems become more autonomous and human review is not always possible.

"It is going to be impossible to always have a human in-the-loop if I want to be autonomous," Loza said. "Use and scale your existing governance process where possible. Because otherwise, you are going to actually limit your potential innovation."

At the USDA, putting those frameworks into practice also requires having a fully developed governance structure or hierarchy, and focusing on employee education and coordination across agencies. Rojas said the department is building AI education into annual employee reviews and sharing best practices through federal CIO and CISO councils.

"We are also developing, as part of the data strategy plan, centers of excellence around the country where farmers and producers are predominantly needed," Rojas said. "[They] need information and agency support."

Investing in the Data Behind AI

Those governance efforts also shape where the USDA and Oakland are directing limited resources: preparing their data for AI and equipping employees to use it responsibly.

At USDA, decades of databases, legacy applications and ad hoc reporting tools complicate that work. Rojas said the department is working across its agencies and with vendors to consolidate, standardize and provide data for reporting and analytics. This can help producers track grants and loans.

"Getting that data into a useful, meaningful datastore is like the number one priority that we had. It seems to finally be gaining traction," Rojas said.

But before organizations can put their information to work through AI, they need to understand where it resides, who controls it and whether it is reliable. That's where subject matter experts come in, to assess data quality and identify AI-generated errors.

And with limited resources, Batalla said Oakland is investing accordingly, putting dollars into data governance tools, policies and employee training before expanding access to AI tools. "Once we had invested in data governance and felt we had a foundation to build on, then we were able to make investments in AI tools," he said.

The city also adopted a hybrid approach. Employees have access to free, general AI assistants that are built into existing platforms, while selected staff receive paid licenses for tools tied to their data and integrated with email, OneDrive and SharePoint. That investment extends beyond licenses as Oakland continues to provide both skills and policy training to ensure responsible AI adoption.

"AI is really changing how information is accessed and used," Loza said, "But it doesn't change the responsibility that our agencies or states have to continue to protect that critical information."

TO LEARN MORE, VISIT CARAHSOFT.COM/BROADCOM

FEDInsider

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

Symantec. by Broadcom | Carbon Black. by Broadcom | carahsoft.

Carahsoft
11493 Sunset Hills Road, Suite 100
Reston, VA 20190
Contact: **Symantec & Carbon Black Team at Carahsoft**

(571) 662-3260
Broadcom@Carahsoft.com
Carahsoft.com/Symantec-and-Carbon-Black
LinkedIn.com/company/Symantec/posts/
LinkedIn.com/company/Carbon-B1ack/posts/

© 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.