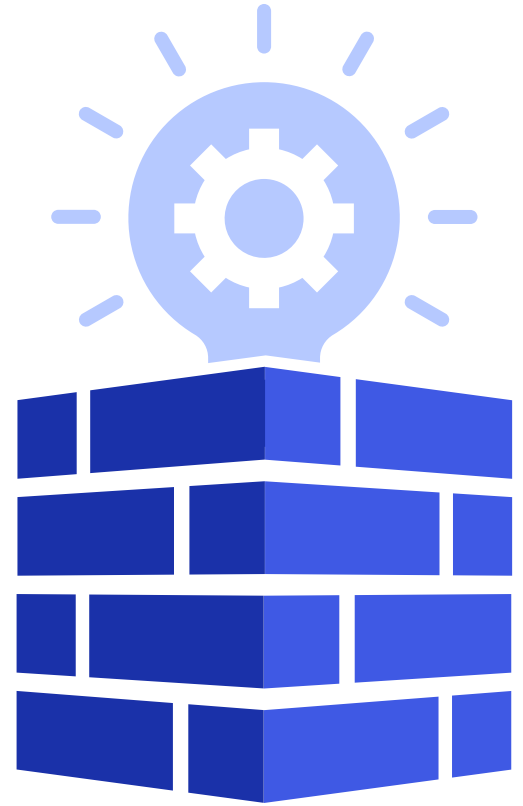


# Building a Secure Foundation for AI Innovation

AI is already reshaping state and local government, enabling new levels of efficiency in constituent services, cybersecurity and internal operations. Now, agentic AI is accelerating that transformation. But as automation expands, it also introduces new risks and complexities.

Secure innovation requires a thoughtful, intentional approach. As AI moves into the mainstream, organizations need greater visibility and control to use it safely and effectively. That makes strong governance essential, especially as AI agents become more capable and autonomous.

At a recent [GovLoop virtual event](#), experts from government and industry offered practical tips for moving safely and effectively into the next phase of AI adoption.



## The Speakers



### Jerred Edgar

Chief Information Security & Operations Officer, Idaho



### David Hinchman

Director, IT and Cybersecurity, U.S. Government Accountability Office



### Ryan Murray

Deputy Director, State Chief Information Security Officer, Arizona Department of Homeland Security, Statewide Information Security and Privacy Office



### Morgan Reed

Distinguished Strategic Advisor, Okta

## Onboard AI the Same Way You Onboard Humans

Arizona has well-established processes for onboarding and offboarding human employees. With the rise of agentic AI, however, governments will see an explosion of machine identities, and those will require a similarly disciplined approach to management, said State CISO Ryan Murray.

Going forward, identity and access management will be a cornerstone of AI governance. Policies and procedures must span the entire technology stack to ensure AI agents access only what they are authorized to access and perform only the tasks they are intended to perform.

“We’re trying to build that into our upcoming policies and procedures: To say that **it really doesn’t matter what the identity is, whether human or machine or agentic, we need to be paying attention to a lot of the same controls,**” Murray said.



## Implement Governance to Manage AI Behaviors

You wouldn't let a brand-new employee loose on your network with a laptop, without having robust oversight in place. Yet organizations may not be applying that same diligence when it comes to AI, Okta's Morgan Reed cautioned.

He pointed to recent data showing that many organizations using generative AI experienced a security incident in the past year. Siloed systems and accumulated technical debt may be partly to blame, as organizations struggle to deploy AI securely across both modern applications and legacy infrastructure. Modernized tools, paired with strong governance and policies, can help agencies innovate securely.

**"If you want good government, you need good governance,"** he said.

In this context, that means ensuring visibility and control over how AI behaves. Employees are already putting AI to work, and software providers are embedding AI agents into a growing number of tools. As a result, agencies need policies that apply the same auditing practices and security-awareness training to AI that they use to manage human behavior.

For example, agencies routinely run phishing tests for their employees, Reed said. "You need to have those same capabilities built for AI."

## Apply Proactive Strategies to Keep AI on Track

In developing governance for the AI-driven era, agencies need to approach AI as they would any other IT investment. Early assessments, evaluations and screenings can help identify potential issues before they arise, said GAO's David Hinchman. Ongoing oversight is just as important. Too often, organizations deploy IT tools, get them up and running, and then move on.

That approach can create unintended vulnerabilities — especially with AI, a technology whose capabilities and behaviors are inherently dynamic and continually evolving. **"If you're not monitoring where this AI is, where it's being used, that's when you start losing track of it,** and you start getting the rogue agents that are out there, because someone built it for something, they sent it out there, then forgot about it," Hinchman said.

Governance should put an emphasis on constant oversight and ongoing controls. This will serve as the foundation for managing the growth and development of AI-driven applications.

## Focus on Developing Both Technical and Soft Skills

There is a human element to AI governance, said Idaho's Jerred Edgar. People need a baseline level of data literacy to understand what information AI is using, the value of that data and the potential consequences when something goes wrong.

Beyond understanding the data itself, AI users must also be able to communicate that understanding, both with one another and with the IT teams enabling these tools. Yet AI can inadvertently weaken those same skills. If users overly rely on AI to draft emails and summarize conversations, it can subtly erode their own ability to articulate their thoughts and ideas.

Because AI can undermine communication, agencies need to pursue professional development that focuses not just on the uses of the tools, but also on the ways in which people interact with one another. **"As we enhance our technologies, we're going to have to put a bigger premium on developing those soft skills between the technical staff and the non-technical staff,"** Edgar said.



*To learn more, watch the [full session on demand.](#)*