MAULDIN & JENKINS
CPAs & ADVISORS

AI Changes the Shadow IT Equation for Governments

By: Jon D. Hightower, CISA, CRISC, CIPT, FAIR | Director, Mauldin & Jenkins

State and local governments have wrestled with the problem of unauthorized devices ever since smartphones, laptops, and tablets gave employees new options for accessing data and systems. This "Shadow IT" issue has long been a concern for security-focused leaders, but the rise of autonomous artificial intelligence agents has turned what was once an annoyance into a significant systemic risk. Unlike standard software, AI agents carry major governance and fiduciary challenges that affect how governments should approach risk management, internal controls, and regulatory compliance.

The Risks of AI With Agency

Today's Shadow IT gremlins present far more complex threats than unapproved laptops or cloud storage accounts. AI agents have, as the name suggests, agency. This means they can observe, learn and act independently – which is part of what makes them so useful. These high-tech entities can deliver meaningful benefits and transform the way governments solve problems, helping with everything from emergency call system automation to predictive maintenance.

But with AI agents freely available, employees can easily install one on any computer, give it access to login credentials and connect it to your applications and data. That's a major problem that introduces critical risks for your government, including:

- **Financial risk:** What happens if unapproved, automated AI agents interact with your government's procurement systems, financial platforms, or accounting systems? If these agents perform unseen actions within the system, they could establish virtually untraceable errors that throw core records and databases into doubt.
- **Regulatory risk:** AI that's neither approved nor allowed can expose governments to penalties and legal recriminations by violating compliance frameworks such as HIPAA, CJIS, and state-specific privacy mandates.
- **Data integrity risk:** Governments can use and process sensitive citizen data in limited ways. Unauthorized AI agents may handle it without leaving an audit trail that specifies sources and distinguishes between allowable and disallowed data. As a result, you may wind up including dirty data in official records.

Addressing the AI Agent Problem

Your IT team works diligently to protect your government entity, but even the most rigorous approach to firewalls and port security won't stop an AI agent that is invisible to the department. A thoughtful approach to governance, risk, and compliance can reduce AI-associated risk of all kinds. Take these four key steps to help protect your organization.

1. **Create a strong policy fit for the AI era.**
   Most government entities are relying on IT policies and internal controls designed well before the advent of ubiquitous AI. It's essential to draft, implement, and enforce an updated policy that meets the new demands of the AI era. Your policy should include:

   - Clear language that forbids employees and vendors from installing any unauthorized AI agent on government computers or hand-held devices.
   - A formal approval process to determine which AI tools are allowed and define the operational tasks they may perform.
   - An access model for approved AI tools that allows the least amount of access needed to perform relevant tasks.

2. **Conduct an AI and Shadow IT risk assessment.**
   Do you know which "unknown but authenticated" devices are letting autonomous AI agents into your systems? Most government entities don't, but these devices often harbor unapproved AI agents that represent significant unrecognized risk. A comprehensive risk assessment by security experts can help you identify security vulnerabilities and oversight gaps. Your assessment should evaluate current workflows and IT asset management strategies, flagging all unknown devices on the network for a thorough investigation.

3. **Manage third-party AI risk.**
   Government entities rely on a growing number of technology service providers that use AI tools. Vendor due diligence can help minimize and mitigate the risk associated with these relationships. Carefully review your service level agreements with AI partners and other vendors that have access to government systems or data. When considering potential relationships with third-party AI providers, explore their policies as well as their track record around data privacy, security controls, and processing integrity.

4. **Maximize algorithmic transparency.**
   Government entities must be able to clearly see how decisions are made. Compromising this ability puts you in an indefensible position during an audit, a public inquiry, or any type of controversy. Ensure that you have human oversight in place and document "human-in-the-loop" controls whenever AI is part of the decision-making process. This rule holds for government systems that use AI to help guide decisions at any level, whether you're determining benefits eligibility or optimizing infrastructure.

Rise to the AI Challenge

AI gives your government entity new opportunities, but it comes with liabilities too. A reactive approach to the risks won't serve you well — or the citizens you represent. An experienced government advisor can help you adopt a strategic posture built on best practices, allowing you to capture the benefits of advanced technologies while meeting rigorous accountability standards.