ATARC | intel

Powered by GovExec

Modernization for Tomorrow: Preparing Government IT Systems for the AI Era

Highlights from a Roundtable hosted by the Advanced Technology Academic Research Center (ATARC) in partnership with Intel Corporation, December 2024

In a recent roundtable discussion, federal experts discussed how agencies are preparing government IT systems for the next era of technology. The conversation focused on the many barriers and challenges agencies face with modernizing existing technology to withstand the innumerable risks associated with AI.

AI Use Cases

Several agencies on the panel have begun deploying generative AI to assist with specific use cases. One agency started using AI to aid with moving a data center into the cloud, but the initiative was halted by leadership for fear of being the first agency to do so. Panelists are optimistic that new leadership will encourage the continuation of AI.

Other agencies are operating entirely in the cloud, which gives them tremendous capabilities to quickly scale in multiple directions and take advantage of FedRamped cloud-based solutions. With the adoption of AI, the agency was able to shorten an acquisition process to 3 weeks, saving over 4,600 manhours.

Another agency on the panel is optimistic about AI's ability to run actual records categorization, while others are using AI as a career pathing tool to support and encourage workforce development. One panelist shared that their agency has used generative AI as a training tool to simulate real-world situations and as a translator. Another agency is using an AI gateway solution to monitor traffic and control access all the way to the endpoint, and to learn patterns for insider threat prevention.

Some panelists are combining AI and ML to learn how to fix complex machines in factories to enhance maintenance and management practices. Several panelists are using AI capabilities for mundane, administrative tasks, such as recording virtual meetings, taking notes, sending follow-up emails, and scheduling meetings.

While some agencies have found success with AI, others have not yet found a strong use case to test its powers. Panelists note that the benefits of generative AI are realized by inputting strong prompts and training the system with clean data. Otherwise, outputs can be unreliable, generic, made up, or biased.

Challenges

> **"Generative AI is the future. It will fundamentally change IT operations in 10 years. What we do today will be gone. Embrace the change and embrace the chaos, because we need to get in front of this now. If we cannot secure generative AI today, the next thing that comes out will take us apart at the seams."**

AI Policy

A few agencies on the panel have formed councils or steering committees to develop AI strategies. The committees are composed of individuals from multiple disciplines to ensure all concerns are heard and weighed. Other agencies do not have formal, documented AI strategies, but operate on the directions set forth by agency leadership.

However, some panelists believe that certain documented AI strategies are not actionable, and are only developed for compliance purposes. In future versions, they hope AI strategies do a better job striking a balance between zero trust and AI innovations.

Others are working on developing AI security policies, but are challenged by the extent of risk associated with AI. With generative AI, a singular risk may be connected to 50 other variations of the same risk, requiring 30 different types of risk mitigation strategies. The risk does not stem from a single point in time, rather it extends to actors, intentionality, the interactions of multiple models, or other factors all together. Panelists note that generative AI cybersecurity risks are fundamentally different from traditional risks, and policies should reflect this new dynamic.

> **“Generative AI is fundamentally different from anything we’ve ever dealt with. It is not only a system, but it's also a user and infrastructure all at the same time. The kinds of risks are very dynamic and spread across the entire spectrum of risk.”**

Panelists point to and recommend MIT’s risk model framework to develop policies that adequately address generative AI risks. They note that, as of now, there are almost 800 known unique generative AI risks, yet leading Federal AI policies account for only 200 of them.

Expanding Attack Surface

The heightened risk stems in part from an expanded attack surface. Panelists discuss the vulnerabilities associated with IoT, remarking on the level of insecurity that currently exists and how AI will only compound that. Panelists also discussed challenges with supply chain visibility, and the risks involved with old devices, chips, or other hardware manufactured by adversaries.

Data Visibility and Security

> **“Things are changing so fast, we don't understand what these AI are doing and what’s leaving our enterprises.”**

One of the chief concerns among agencies is not knowing exactly how Software as a Service (SaaS) providers are using government data. Panelists note that there is a wide misconception among users that government and personal data is secure when sending emails or using FedRamp software with built-in AI capabilities. One panelist explained that exchange online protection gateways, which scans emails before entering government networks, are solely managed and in control of email providers. Sending unencrypted emails through encrypted tunnels does not protect government data.

Panelists also acknowledge challenges with cleaning data to be used in AI models. For some, they are working to clean data sets built on varying rule sets. Some agencies on the panel admit they have very poor data governance, and the data pillar of zero trust is their biggest current challenge.

Hallucination and Bias

> **“What makes generative AI generative AI is its ability to create its own data.”**

Panelists discussed the risks associated with AI and decision making. One panelist noted that generative AI has a 2% hallucination rate, which underscores the importance of checking outputs. These concerns stem from not knowing how generative AI models are taught, who taught them, or what data was used in training them. Users may give an AI valid data, but based on how it was trained, may generate biased information.

One panelist shared a real example of how AI bias can impact hiring decisions for years. One person could insert a small line of code, among millions, to instruct the AI that reviews HR applications to overlook applicants based on certain qualities. Agencies could easily miss this, and unknowingly be engaging in unfair hiring practices.

Final Thoughts

While some agencies have embraced AI and identified valuable use cases, others are still exploring and proceeding with caution as strategies and policies continue to be developed. Continued collaboration and knowledge sharing will be crucial as agencies continue to modernize their systems in the AI era.

LEARN MORE AT: INTEL.COM/PUBLICSECTOR