Shaping Federal Governance: The Evolution of Generative AI Integration

Highlights from a Roundtable hosted by the Advanced Technology Academic Research Center (ATARC) in partnership with INDR

The digital revolution is defined as the shift from mechanical and analog to digital electronics, which already happened, the Federal government is reaching a critical inflection point as the use of generative artificial intelligence (AI) is explored and interrogated.

At a recent roundtable discussion, Federal IT officials and industry experts explored the vast potential of generative AI in government, while underscoring the risks of the new technology. Roundtable Federal IT participants also shared specific AI use cases, demonstrating AI's powerful ability to drive results and save resources.

Current State of Generative AI in Federal Agencies

With the exception of one agency on the panel, all have used generative AI to a limited degree. However, they all share a genuine concern about the risks of AI in government and are approaching it with controlled caution. Unlike previous technology adoptions, generative AI is transforming the IT industry in the private and public sectors in profound ways, virtually overnight, and cannot be ignored.

Some federal agencies have already provided guidance to employees on the use of AI. Others have issued specific user behavior agreements for AI use, while others have altogether blocked generative AI from computers using firewall-like protections. For some, the risks of AI to the agency outweigh its current benefits. Ultimately, panelists are awaiting top-down AI guidance before venturing too deeply into the new technology.

Data Concerns

The heightened caution is warranted for many reasons. Roundtable participants overwhelmingly agree the risk to data collection and use is a chief concern. They're particularly concerned with data spillage and government data being used to train AI models.

Panelists questioned how government data should be consumed by AI models, who the data should be shared with, and the role of third-party vendors in using government data for the purpose of generative AI. Moreover, many government agencies do not have sufficient data to train their own AI models effectively and securely. The lift to create data for AI models to learn from will be significant.

Agencies are also increasingly more concerned with inaccurate AI outputs that can put agencies at risk of serious liability. Panelists remain distrustful of AI's ability to represent the government in an appropriate and legal manner. In one A/B test, an agency's AI test model gave a humanistic, emotive response to a customer inquiry, rather than a factual one. In this instance, the agency could not control or rely on AI to represent the agency accurately and appropriately.

One roundtable participant encouraged agencies and industry partners to collaborate and train AI models on trusted, government data. Ensuring the government remains the most trusted source of certain information is critical. Agencies are actively seeking ways to validate the accuracy of models and detect any deviations that might influence the precision of AI outputs. Additionally, they are exploring methods to promptly identify and respond to any signals indicating changes in the AI model that could impact the integrity of the information provided.

Ultimately, agencies are awaiting guidance and FedRamp guardrails before venturing too far into generative AI. Panelists reiterated throughout the discussion that this technology is rapidly changing and will likely be consolidated in the near future. As such, agencies should not rely on one solution or vendor too heavily.

> **“It's going to help us. It's going to do things for us. But we're going to have to evaluate it and start to decide if we trust its output.”**

Generative AI Use Cases in Federal Government

While panelists will not use public, open-source generative AI due to privacy, security, and liability concerns, many organizations have started utilizing generative AI in specific, controlled situations using reliable government data. Generally, this is the approach panel experts encourage agencies to take.

- **Scientific predictions.** Agencies whose mission is to advance science are interested in the transformative potential of AI in a range of scientific and engineering tasks, including predictions and software modernization. However, they do not yet completely trust the conclusions reached by using certain AI models.

- The scientific community is also concerned about access to AI model training materials, specifically copyrighted scientific literature and whether it will be considered fair use. Agencies question whether openly sharing data in this manner will create unintended consequences.

- **Enhanced customer service.** Agencies are especially excited about the potential for AI to provide personalized, on-demand customer service. Many agencies struggle to manage the volume of customer inquiries flooding phone lines and inboxes each day. An AI tool that could accurately respond to complex customer inquiries will transform many agencies.

- **Survey operations.** Agencies that survey citizens can benefit from the predictive nature of generative AI when generating and analyzing survey data. However, agencies are concerned with the relevancy of responses. An agency on the panel tested the responses of the major AI services on the market. Each provided a different response to the same query.

- **Enhanced cybersecurity.** With the advent of AI, threat actors can target attacks with surgical precision. Agencies are working to deploy equally sophisticated cybersecurity measures within the year.

- **Potential for more tech talent.** One panelist suggests that by introducing AI, the bar is lowered for employees to enter the field of technology. Instead of having to learn and understand complex databases, employees will be able to ask plain language questions. They believe staff will become more involved with technology because of the flexibility AI gives to cybersecurity.

- **Promoting innovation.** Some agencies anticipate harnessing AI to help people move beyond searching for information and to provide access and formulate new ideas.

- **Analyzing vast amounts of data.** One agency used AI to train models to identify anomalies in a large database, saving an estimated 35,000 staff hours.

Other Use Cases

- Legacy code conversion
- General email and letter correspondence

> **“We see generative AI in our future, but we're being cautious. Right now, public AI is a data exfiltration path.”**

Industry Perspective

> **“The last six months, the last three months and the last month – the advancements we have made in this technology have been tremendous.”**

Industry representatives on the panel predict there will be considerable consolidation of AI capabilities in the near future, and key players in AI will emerge. Service providers are continually navigating changes, in regards to both policy and technology, and are working to future-proof their implementation as the target continues to move.

Like government agencies, industry partners are also concerned with the explainability, reliability and trust of AI outputs. One partner at the roundtable shared how they approach this challenge by marrying their own targeted data with large language models (LLMs). They assign confidence levels to the outputs depending on how much of their own data is included in the response. Sharing this information in a transparent way will likely become an industry standard moving forward.

Looking to the Not-So-Distant Future

> **“Everyone wants AI, and they want it now. They're just not quite sure where they actually want to leverage it.”**

While this is certainly not the first time agencies have implemented new technology, there are significant differences in how agencies will be implementing AI. Although cloud adoption has been slow across agencies, one roundtable participant believes agencies will not have the option to drag their feet when it comes to AI. AI technology is going to be integrated and embedded into the technologies agencies are already using, and it will shape the industry in terms of competitiveness.

Government agencies should undergo a very careful evaluation of what it takes to use generative AI properly and to vet the results to then incorporate them into workflows. One panelist cautions agencies to first articulate their intent with AI. Is it to use AI as a construct to receive budget money, or is AI the optimal approach to a solution? While AI is full of promise, agencies should consider what their business goals are, and how AI will fit into and enhance existing processes. In some instances, agencies may not have the processes in place to support AI use.

An industry partner at the roundtable recommends a focused approach. Finding specific, low-risk ways to leverage AI can offer quick wins to agencies looking to advance. They recommend that agencies write more specific requirements so service providers understand the desired outcomes.

As the opportunity to innovate with AI increases, agencies and industry partners alike will need a safe and reliable playbook to guide successful AI implementation. NIST is working diligently on developing an AI Risk Management Framework. The framework is similar to the cybersecurity framework but will help agencies manage the unique risks associated with AI systems. This framework is also unique in that it is a socio-technical risk management framework, which marries the social and technical risks of AI together. NIST aims to produce a draft available for public comment in late 2023. In addition, leading global government thought leaders in the U.S. and U.K have started to collaborate on developing guidelines on how to securely develop and deploy AI systems. The voluntary guidelines provide a set of recommendations to organizations about how to develop and build AI systems with security in mind. The high level framework provides guidance across design, development, and deployment and secure operation and maintenance of AI systems.

Final Thoughts

Roundtable participants closed the discussion with a reminder to consider the human impact of this new technology. While there is considerable noise around AI, we still do not yet understand the impact AI will have on workers. People may be hesitant about AI efforts because they believe it will eventually replace them. The onus is on agency leaders to ensure employees understand both the possibilities and limitations of AI, and to reinforce their value in the workplace.

Leaders should also be aware of the positive impact AI will have on accessibility, especially those with different abilities. As one panelist noted, “the potential for improving the lives of people that have been historically underserved is amazing”.

LEARN MORE AT:

HTTPS://WWW.INDR.COM/