FROM AI ADOPTION TO DECISION ADVANTAGE

Federal agencies can turn AI into a mission force multiplier by strengthening their data foundations, enabling responsible experimentation, and adapting governance, security, and investment practices for a faster operating environment.

Federal agencies have moved quickly to explore artificial intelligence (AI), launch pilots, and establish initial governance frameworks. The next stage will be more demanding: turning isolated experimentation into trusted capabilities that improve decisions, accelerate operations, and perform reliably at mission scale.

That transition was the focus of a recent roundtable discussion with Leidos and federal agency leaders spanning IT, AI, cybersecurity, innovation, and data. They identified significant opportunities to use AI to synthesize information, identify patterns, streamline routine work, and place better information in the hands of decision-makers. They also emphasized that technology alone will not create lasting advantage.

"The question isn't whether AI has a place in government. It's how we make it work," said Rob Linger, Vice President of Information Advantage at Leidos.

Making AI work requires agencies to address the quality and availability of their data, the strength of their security and governance practices, the readiness of their workforce, and their ability to align investments with meaningful mission outcomes, the experts noted.

BEGIN WITH THE OUTCOME

AI discussions often begin with models, tools, and features, but agencies will get greater value when they start with the decision or operational outcome they want to improve, agency leaders said.

In some cases, AI can help analysts search and synthesize large volumes of information in a fraction of the time previously required. In others, it can identify relationships across data sources, help teams prioritize risks, or automate portions of repetitive workflows. More advanced capabilities may eventually observe changing conditions, recommend actions, and execute approved tasks under human oversight.

The common thread across these applications is the ability to shorten the distance between information and action.

This mission-centered approach can also help agencies decide where AI does not belong. Not every process needs an AI component, and introducing one without a clear operational purpose can add cost, risk, and technical debt, leaders warned. Agencies need to identify where AI can make a measurable difference and where established tools remain sufficient.

"The organizations that create lasting advantage won't necessarily be the ones with the newest model," Linger said. "They'll be the ones that use the right tools at the right time to achieve the outcomes they need."

TREAT DATA READINESS AS AN OPERATIONAL PRIORITY

The discussion consistently returned to data as the central constraint on AI adoption. Agencies possess enormous volumes of potentially valuable information, but much of it remains fragmented across systems, offices, inboxes, shared drives, and repositories governed by different access rules.

Some data is duplicated. Some lacks common definitions or consistent tagging. Other information may be retained because of longstanding policy even though teams rarely use it. In many cases, agencies do not fully understand what data they possess, who owns it, or which rules should govern its use.

"For AI to work, the data has to be organized, trusted, connected when needed, and ready for the mission," Linger noted. "Access to models is not the differentiator. The differentiator is how well an organization manages and uses its data."

Agencies do not need to clean and consolidate every historical data source before launching targeted AI use cases. A more practical strategy is to improve data governance alongside those use cases, the experts advised. As teams bring selected data into an AI-enabled workflow, they can establish ownership, define access requirements, apply common terminology, and determine how the information should be maintained.

That incremental approach can create immediate mission value while gradually improving the quality, consistency, and usability of agency data. It also allows agencies to apply stronger governance to newly created data from the outset.

REPLACE STATIC GUARDRAILS WITH VISIBLE, GOVERNED ACCESS

Federal employees are already encountering AI in agency software and online tools they use outside of work. When AI capabilities at work are unavailable or too restrictive, users may turn to personal devices or unapproved tools to complete their work.

Providing approved tools within a protected environment gives agencies greater visibility into AI use and a better opportunity to manage security, privacy, and compliance risks. It also creates valuable operational insight, leaders said. By observing how employees use AI, agencies can identify common needs, detect recurring workflows, and determine where a purpose-built capability could benefit a broader group.

Governance, therefore, should make appropriate experimentation possible while maintaining accountability. It should define which data can be used, which actions require human approval, how outputs will be reviewed, and how system activity will be logged and monitored.

PREPARE THE WORKFORCE TO USE AI EFFECTIVELY AND SAFELY

AI fluency and comfort vary greatly across the federal workforce, roundtable participants noted. Early adopters working on small, well-defined projects can demonstrate value and build confidence. Successful applications can then inform training, governance, and broader deployment.

Back-office functions such as acquisition, finance, human resources, and legal operations warrant particular attention. These teams help determine how quickly agencies can purchase, authorize, fund, and oversee AI capabilities. Giving them practical experience with approved tools can help them understand the technology, address concerns, and participate effectively in agency adoption.

AI education should reach employees across job functions rather than remain concentrated within technical teams or isolated organizational units, leaders advised. Agencies also need to create an environment in which employees can report mistakes or concerns without assuming that missteps will result in punishment. A punitive approach may limit the visibility agencies need to manage AI responsibly.

INTEGRATE AI WITH CYBERSECURITY

AI changes the security model because useful systems often require access across boundaries that agencies have historically used to isolate networks and data. Generative AI applications and autonomous agents may need to retrieve information from multiple environments, interact with other systems, and act on behalf of users.

"AI and cybersecurity have become inseparable," Linger said.

Agencies will need stronger visibility into what AI systems can access, which identities they are using, and what actions they are authorized to perform. Zero trust principles provide a useful foundation: verify users, devices, applications, and machine identities; enforce least-privilege access; and continuously evaluate behavior, leaders noted.

AI may also help agencies strengthen those controls. It can assist with data inventory, tagging, and classification; identify relationships among vulnerabilities and likely paths of lateral movement; and help security teams synthesize more threat information than analysts could assess manually. Used with appropriate safeguards, AI can give agencies greater insight into their environments and support more informed risk management.

BUILD AN OPERATING MODEL FOR SCALE

Sustained AI use to support agency missions will require agencies to adapt their budgeting, acquisition, infrastructure, and performance measurement practices. Rapidly changing token consumption, pricing models, and computing requirements can make costs difficult to predict within established planning cycles.

Agencies therefore need greater visibility into both AI consumption and results, the discussion revealed. Tracking usage and costs by project can help leaders establish appropriate guardrails and make more informed decisions about where computing resources should reside. Establishing baseline measures can also help agencies compare performance before and after implementation and determine whether a capability is producing sufficient mission value.

The path forward is unlikely to be a single enterprise deployment or a fixed end state. Agency experts described AI adoption as an ongoing journey built through small projects, measured results, and continued learning. Agencies will carry those lessons into new implementations as capabilities, costs, and risks continue to evolve.