FEDERAL NEWS NETWORK

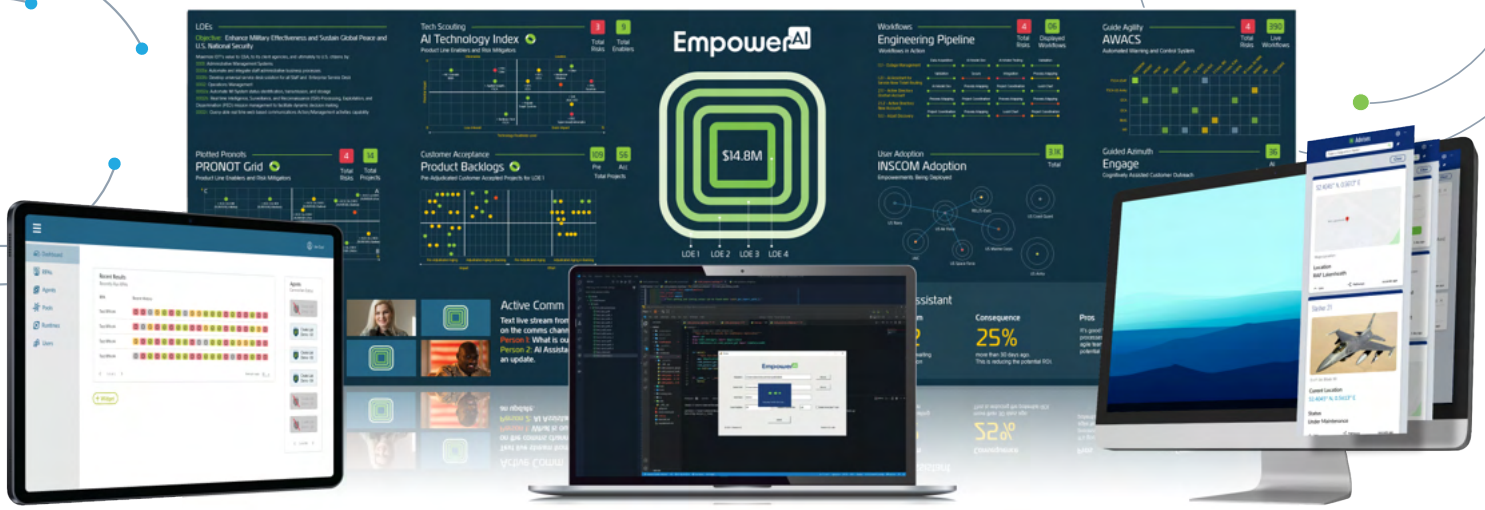
EXECUTIVE BRIEFING SERIES

How to build transparent and effective AI systems

BROUGHT TO YOU BY EmpowerAI

Empower AI

Elevate the Mission



AI Built For Government Missions

Proven. Scalable. Secure.

Learn more at www.Empower.ai

2x+ Return on Investment	**90%** Savings on staff time and resources	**5x** Faster than human work	**98%** Productivity increase and improved security

How to build transparent and effective AI systems

BY TOM TEMIN

Artificial intelligence projects in the federal government range as widely as the agencies' missions themselves. Differing as their AI applications might be, all AI practitioners face common challenges — namely, how to prioritize investments in AI, how to best stage and otherwise carry out AI projects, and how to ensure acceptance by the intended beneficiaries of AI and its results.

To glean current best practices for managing AI in government, we asked a panel of federal and industry experts about how they are choosing, hosting and managing the technology. A consistent theme emerged: IT organizations must keep close watch on mission support so as not to spread resources and expertise too thin.

Robert Keisler, director of data science and AI at the Naval Information Warfare Center Atlantic, summed up that thinking. Where to start in the first place depends on the strategic priorities as expressed in military strategies, like the Chief of Naval Operations Navigation Plan or the Marine Corps Force Design 2030, he said.

Knowing the top goals, his center then takes a mission engineering approach to AI, Keisler said. That leads to identifying the highest priority tasks and the metrics for measuring success in applying AI to them. From there, the center team decides whether to use industry for a particular project or to tackle it in house.

PANEL OF EXPERTS

Gil Alterovitz
Director, National Artificial Intelligence Institute, Veterans Affairs Department

Edmon Begoli
Head, AI Systems R&D Section, Oak Ridge National Laboratory, Energy Department

Eric Ewing
AI Lead, IT Modernization Center of Excellence, General Services Administration

Donald Hornback
AI Program Manager, Intelligence Advanced Research Projects Activity, Defense Department

Robert Keisler
Director, Data Science and AI, Naval Information Warfare Center Atlantic

Gabriel Perdue
Senior Scientist, Fermilab Quantum Institute, DoE

Allen Badeau
Chief Technology Officer, Empower AI

Success must tie back to the mission, he advised. "Otherwise, AI just becomes 1,000 points of light. We [would] never really get the actual impact we want to get."

AI return on investment factors

The panelists also said that traditional measures of IT return on investment — for instance, lower storage lifecycle costs with a new hardware subsystem — apply less to AI investments than the measure of mission effectiveness.

For Eric Ewing, artificial intelligence lead in the IT Modernization Center of Excellence at the General Services Administration, that means helping agencies that want to establish AI projects make those connections to goals and deliverables.

"We're looking at what the [customer] agency mission is, what the agency priorities are at the moment, and then mapping down to well-wrought areas where AI has can have impact," Ewing said. Often, those things involve data that is "highly structured or highly regulated — think financials, think grants data — and then areas within those programs that are being prioritized."

With that level of detail, Ewing's group is able to help an agency apply AI technology "in a way that that solves an inherent business problem, or to improve customer or citizen experience," he said.

Plus, Ewing pointed out, "Looking at ROI in the federal government is an interesting thing. It's not always financial ROI we're looking for. We also want to make sure we're improving the way the federal government operates."

Impact on operations is the best way to measure AI return on investment, said Allen Badeau, chief technology officer of Empower AI, a company that offers AI solutions on-premise or in the cloud for the federal government.

"Looking at ROI in the federal government is an interesting thing. It's not always financial ROI we're looking for. We also want to make sure we're improving the way the federal government operates."

— Eric Ewing, AI lead, GSA's IT Modernization Center of Excellence

He said agencies look at impacts according to their missions. For example, many agencies want to use AI to improve customer service, whether for employees or for the public. The impact in this context, Badeau said, "can be the optimization of operations and the user satisfaction associated with that service desk." In a military application, more accurate targeting might be the measure. And in fee-for-service agencies, Badeau said, the ROI measure might in fact be a more traditional financial metric.

Badeau added that agencies should not overlook the application of AI to information technology operations themselves. One ripe area here is modernizing or replacing legacy code. Agencies have large blocks of, say, COBOL that is difficult to maintain, yet the logic of which remains crucial.

"Looking at the user experience, looking at how you can augment a human programmer's capability to modernize code," Badeau said, "is an area of research that industry is really pushing very hard. And I know that we are as well."

Mission-focused AI

That's exactly how agencies are prioritizing their AI investments.

For example, the Veterans Affairs Department has established a Digital Command Center. Gil Alterovitz, director of VA's National Artificial Intelligence Institute, described the command center as a platform for vetting AI modules for applicability to important questions related to veteran care, as suggested by VA's own practitioners.

Meanwhile, at the Energy Department's Fermilab Quantum Institute, Senior Scientist Gabriel Perdue is concentrating on the efficacy of AI for components of quantum science.

"If you're using AI to empower a measurement, for example, we need to measure, 'Are these quantities consistent with the truth with a capital T?' " Perdue said. As for ROI, here the criteria blend cost and mission effectiveness, especially given the potential costs of certain quantum experiments.

"Properly simulating a quantum computer is exponentially expensive," Perdue said. "The closest I could get to financial return would be to think about how much it would have cost to try to do a project. Very often, it's the case that the most interesting ones are the projects that really weren't even remotely feasible without AI."

When it comes to establishing an AI project, once the agency has established where to apply it, it also must choose from an array of ways to proceed.

Alterovitz said VA has had success with several approaches. A cooperative research and development agreement (CRADA) resulted in software that can predict, and therefore help doctors prevent, acute kidney injury. For its digital command center, VA acquired a commercial AI product. VA's own developers may write an algorithm that staff integrates into and extends the functionality of an existing piece of equipment, such as an imaging machine.

> "We have operations across the entire spectrum. We have warfighting, we have business, we have logistics. The ability for AI to impact all of those things is enormous, but it's also so different across every type of application."
>
> **— Robert Keisler, Director of Data Science and AI, Naval Information Warfare Center Atlantic**

AI: Buy it or build it?

In short, Alterovitz said, "you can buy it, you can build it, and you can also kind of collaborate."

Technical approaches in the military vary according to domain.

"In the Defense Department, we have operations across the entire spectrum. We have warfighting, we have business, we have logistics," Keisler said. "The ability for AI to impact all of those things is enormous, but it's also so different across every type of application."

In logistics, he said, "more often than not, we can pull things off the shelf" and acquire commercial AI products.

> "Looking at the user experience, looking at how you can augment a human programmer's capability to modernize code, is an area of research that industry is really pushing very hard."
>
> **— Allen Badeau, CTO, Empower AI**

In the warfighting domain, Keisler said, "outside of some newer vendors that have started to show up, those techniques are not things that we can get off the shelf. I think that becomes more of a technical challenge for us."

Training AI and machine learning algorithms in federal use also requires a careful strategy.

Donald Hornback, AI program manager at the Intelligence Advanced Research Projects Activity (IARPA), noted the vulnerability of algorithms to the training data. The wrong data can result in erroneous or biased results.

Hornback recommended that when acquiring commercial AI products, agencies know the "provenance of those models that have been trained, the data that they've been trained on and what is the impact on the correctness" of the outcomes. Sometimes, Hornback said, use of an open source AI model that was trained in a commercial context may require retraining with data the agency considers more trustworthy.

It's also important to know any security risks associated with the application programming interfaces an agency uses on its data, he said.

Why? "So that you know them to be correct or whether it's been manipulated in some sort of malicious or adversarial way," Hornback said. For situations where no commercial product exists for a federal application, there's the Oak Ridge National Laboratory, offered Edmon Begoli, head of the lab's AI Systems R&D Section.

The lab's researchers work to "advance the state of the art in domains that are not covered by research that is happening outside the federal sector, and to translate and evaluate technologies for their validity and effectiveness," Begoli said. And his group also tests the reliability, validity, robustness and resilience of AI in federal domains such as cybersecurity and in commercial products that incorporate AI in the way that they work.

Begoli cautioned federal practitioners that many AI products are trained in commercial contexts far removed from anything applicable or even valid in a federal setting.

TikTok or Snapchat preferences or fast food delivery optimization are often the most common ways regular citizens encounter AI, he said.

The AI cybersecurity challenge

In government, "we deal with serious matters. AI is vulnerable. AI is exploitable, and I believe that AI is facing the same kind of problem that software faced 20 years ago, when we discovered this thing of cyber offense and cyber exploitation," Begoli said.

Just as agencies are seeking visibility into software supply chains for purposes of cybersecurity, so must they also ensure the transparency and auditability of AI products, the panelists said.

The challenge, in part, stems from the reality that standards for AI are still maturing, GSA's

Ewing noted. "As those common standards are being developed, we need to have good understanding, and good management and accountability functions, on the AI systems that we develop," he said, adding that so-called black-box AI systems lacking transparency pose the danger of producing unintended outcomes.

To ensure that doesn't happen "requires us to develop interdisciplinary teams for artificial intelligence development and deployment," Ewing said. Bringing in human-centered design, data capture and database management experts "will enable us to build an effective and transparent tool."

> "AI is vulnerable. AI is exploitable, and I believe that AI is facing the same kind of problem that software faced 20 years ago, when we discovered this thing of cyber offense and cyber exploitation."
>
> **— Edmon Begoli, Head, AI Systems R&D Section, Oak Ridge National Laboratory**

Discover more about how the power of AI can help solve complex government challenges

Watch and listen to our Federal Executive Forum on ML and AI in Government featuring federal leaders from the Air Force and Government Accountability Office.