

-  [Edit article](#)
-  [View stats](#)
-  [View post](#)



Why the ACT-IAC Emerging Technology and Innovation Conference 2026 Felt Different This Year



John Binks, PMP®, AWS-CCP, AMA-CPM 
Award-Winning / Best-Selling Author | Federal Growth & Business Development Executive | Federal Systems Integrator...



May 16, 2026

The American Council for Technology and Industry Advisory Council, ACT-IAC Emerging Technology and Innovation Conference 2026, made one thing clear: federal technology conversations are moving from experimentation to execution.

The conference, held May 14–15, 2026, near Washington, D.C., drew several hundred Federal government and Industry professionals and focused on the issues, challenges, and opportunities facing government and industry as emerging technologies reshape mission delivery. Sessions emphasized artificial intelligence, cybersecurity, secure modernization, quantum technology, and practical implementation across federal environments.

What stood out most was not the technology hype.

It was the realism.

Across the sessions, the recurring question was no longer, “Should the government use AI?” The question was, “How do we deploy AI securely, responsibly, and in a way that actually improves mission outcomes?”

AI Is Moving From Pilots to Practical Mission Use

One of the strongest themes was the need to move beyond theoretical AI conversations.

In the AI and cybersecurity discussions, panelists emphasized that agencies need practical pilots, not more slide decks. The focus was on identifying specific problems AI can solve, understanding existing tools, identifying capability gaps, and working with vendor partners to address those gaps.

That is the right shift.

Federal agencies do not need AI for the sake of AI. They need AI that helps reduce risk, improve decision-making, strengthen cybersecurity, process data faster, and support the workforce.

The best AI use cases start with a mission problem, not a product demo.

Cybersecurity and AI Are Now Interdependent

The cybersecurity panels were especially important.

Panelists discussed AI's ability to improve defensive cyber operations by reducing false positives, predicting attacks, detecting vulnerabilities, improving response times, and supporting a more unified view of the threat landscape. They also stressed that AI must work alongside core cyber practices such as zero trust, continuous monitoring, and basic "blocking and tackling."

That point matters.

AI can make cyber teams faster and more effective, but it does not replace strong fundamentals. Agencies still need sound architecture, clear governance, identity controls, trained personnel, and disciplined risk management.

AI may help defenders move faster.

But attackers are moving faster, too.

Several panelists noted that bad actors are already using AI effectively, which means federal cyber teams must adapt quickly, make risk-based decisions, and avoid being trapped by outdated processes.

Zero Trust Is Becoming an AI Conversation

Zero trust also came up repeatedly.

The interesting part is that zero trust and AI are now becoming connected conversations. Zero-trust environments generate enormous amounts of telemetry, access data, behavioral signals, and policy events. AI can help analyze that data at speed.

At the same time, AI systems themselves need to be governed with a zero-trust mindset.

That means agencies should think carefully about:

1. Who can access AI systems?
2. What data can those systems use?
3. How outputs are validated
4. How models are monitored
5. Where human review is required
6. How AI-driven decisions are logged and audited

"Never trust, always verify" applies to users, devices, networks, models, datasets, prompts, and automated workflows.

That is a major evolution in federal cybersecurity thinking.

AI Governance Cannot Be an Afterthought

Another theme that came through strongly was governance.

Panelists discussed the tension between agility and control. Agencies want to deploy AI quickly, but they also need governance policies, clear boundaries, transparency, accountability, and lifecycle controls. The sessions also highlighted the need to integrate AI early in development cycles to prevent mistakes rather than trying to bolt on security and governance later.

That is a lesson the government has already learned from cloud modernization.

If governance comes too late, agencies end up retrofitting controls after systems are already in production.

With AI, that risk is even higher.

The better approach is to build governance into the front end of AI adoption through clear use cases, risk scoring, model validation, testing, security controls, and human accountability.

Workforce Transformation May Be the Hardest Part

The Federal AI Transformation Panel highlighted a point that often gets overlooked: culture and change management may be the biggest barriers to AI adoption.

According to the panelists, there is a need for transparency, training, multiple learning formats, and clear communication between government and industry. They also emphasized that success metrics should go beyond cost, schedule, and compliance to include mission impact, operational resilience, and measurable service improvements.

That is exactly where many AI efforts will succeed or fail.

Federal employees do not need vague promises about transformation. They need practical training, clear guidance, safe spaces for experimentation, and leadership that explains the "why."

AI literacy is becoming a core workforce requirement.

Not everyone needs to become a data scientist. But leaders and employees do need to understand what AI can do, where it fails, how to question outputs, and when human judgment must remain in control.

Shared Services Could Help Scale Emerging Technology

The shared services discussion added another important angle.

Panelists emphasized the need for clear vision, executive buy-in, governance, stakeholder alignment, trust, and interoperability. They also discussed shadow IT as a signal of unmet needs rather than simply a compliance problem.

That point deserves more attention.

If users bypass official systems, it often means the official systems are too slow, too hard to use, or do not meet mission needs.

Shared services can help agencies scale AI and emerging technology, but only if they are designed around real agency demand, clear value, and trusted delivery.

Otherwise, shadow AI will become the next generation of shadow IT.

Quantum Is Moving From Theory to Use Cases

The quantum technology panel also stood out.

The panel titled “Schrödinger’s Roadmap: Sorting Quantum Hype from Federal Reality,” with participants from D-Wave Quantum, NASA, Montana State University, and federal quantum policy leadership.

The discussion focused on practical quantum use cases, including missile defense, telecommunications network optimization, logistics, police resource optimization, GPS improvement, time transfer, cloud-based access to quantum systems, and post-quantum encryption risks.

That was an important reminder: quantum is not just a future science topic. Federal agencies need to prepare now for workforce needs, encryption risks, and mission-specific applications.

The smartest approach is not to chase quantum hype. It is to identify practical use cases, build workforce capacity, and understand where quantum may create operational advantage.

NASA Offered One of the Best Real-World AI Examples

One of the most compelling presentations came from NASA’s Dr. Troy LeBlanc.

He discussed the massive growth of space exploration data, including physical film, still photos, mission imagery, and operational data from human spaceflight. He described AI’s role in cataloging, analyzing, validating, and distributing mission imagery while preserving public trust in the authenticity of images.

That is a powerful example because it shows AI being applied to a real mission problem.

NASA is not just asking how AI can make work faster. It is asking how AI can support mission control, improve data management, help operators make safer decisions, and protect trust in public information.

That is the kind of AI use case the government needs more of.

The Bottom Line

The ACT-IAC Emerging Technology and Innovation Conference 2026 reflected a more mature federal technology conversation.

The focus is shifting from awareness to execution.

From pilots to operations.

From tools to mission outcomes.

From AI excitement to AI governance.

From cybersecurity theory to operational resilience.

The agencies and industry partners that succeed will be the ones that can bring these pieces together:

1. Clear mission use cases
2. Practical pilots
3. Strong cybersecurity
4. Responsible AI governance
5. Workforce readiness
6. Trusted shared services
7. Measurable outcomes
8. Human accountability

AI may be the headline, but trust, governance, cybersecurity, and execution will determine the results.

Note: The American Council for Technology and Industry Advisory Council, known as ACT-IAC, is a 501(c)(3) nonprofit educational organization focused on improving government through the smart and innovative use of technology.

ACT-IAC serves as a trusted, objective, and ethical forum where government and industry leaders can connect, collaborate, and share ideas. It is widely recognized as one of the leading public-private partnerships in the government technology community. It has been described as a strong example of how government and industry can work together effectively.

If you enjoyed this article, be sure to share and repost!

Remember, the bots are getting smarter, but you're still the boss! ©

Copyright © 2026 John Binks / Bots & Bosses LLC, All Rights Reserved

#GovCon #ArtificialIntelligence #FederalIT #Cybersecurity #ZeroTrust
#ACTIAC #EmergingTechnology #GovernmentInnovation
#DigitalTransformation #AI #Leadership #FederalGovernment
#QuantumComputing #SharedServices #GovTech #Vibrint #JohnBinks
#BotsAndBosses

Comments



3



Like

Comment

Share

Add a comment...



No comments, yet.

Be the first to comment.

[Start the conversation](#)



John Binks, PMP®, AWS-CCP, AMA-CPM

Award-Winning / Best-Selling Author | Federal Growth & Business Development Executive |
Federal Systems Integrator (FSI) | AI & Emerging Technology | Public Speaker / Podcaster |
Former FEMA Technology Executive