



CHAIRMAN'S NOTE

Dear Friends,

The hot topics continue to be AI, Service Delivery and the role of Cybersecurity in establishing guardrails to ongoing security breaches that impact data integrity and National Security. Oversight and accountability are critical.

In this issue of ActioNews, we cover the use of Agentic AI, moving from experimentation toward enterprise adoption. The NIST AI Agent Standards Initiative recognized that AI agents capable of autonomous actions require standards that support secure operations and interoperability across the digital ecosystem. The recent National Security Presidential Memorandum on AI directed the national security enterprise to accelerate AI adoption in alignment with these objectives and initiatives.

October is Cybersecurity Awareness Month with a theme of "Securing the Next 250". Cybersecurity awareness has emphasized "Think Before You Click". Now we must also "Think Before We Prompt" and "Verify Before We Trust" as the use of AI Tools can expose sensitive information and propagate misinformation.

Vigilance and Diligence are key in navigating the waters that lie ahead.

Best Wishes for the Fall Season!

Ashley W. Chen
Founder & CEO

IN THIS ISSUE

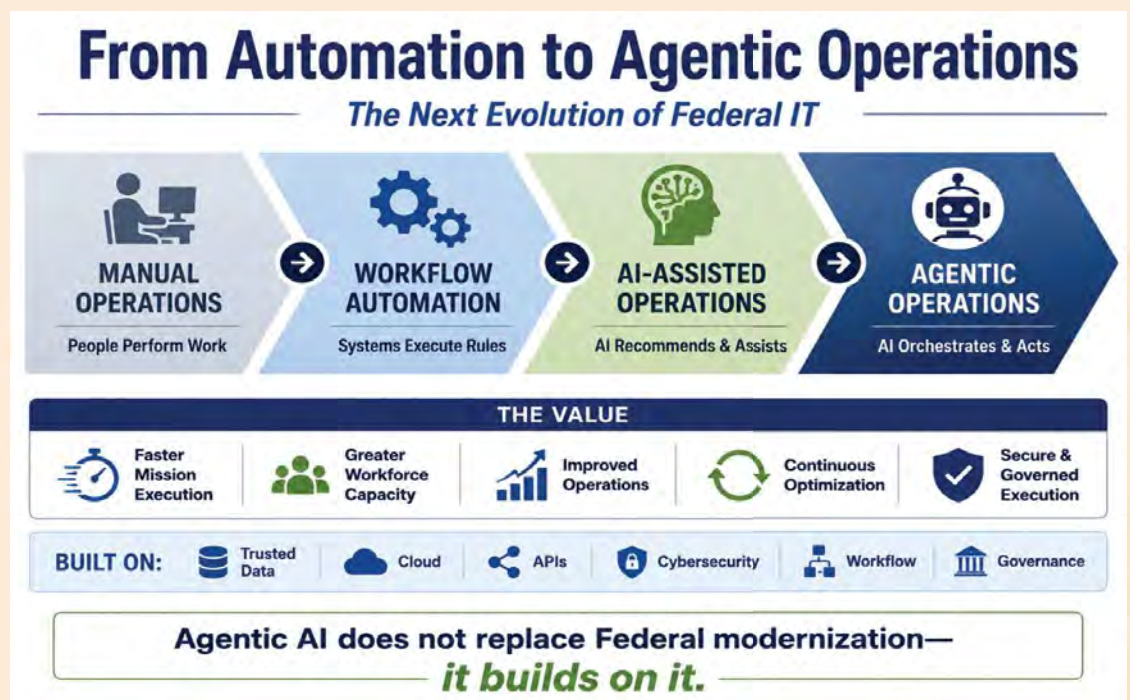
Advancing Federal IT 1
Securing the Next 250 4

Turning **VISION** into **ACTION**®

Advancing Federal IT from Intelligent Automation to Secure, Governed Mission Execution

By Eric Chasteen, Senior Solution Architect

Federal agencies have spent years automating repetitive tasks, modernizing applications, moving workloads to the cloud, improving data access, and implementing digital workflows. These investments have improved efficiency, but they also create the foundation for the next evolution of Federal IT: Agentic AI and Agentic Operations.



Traditional automation follows predefined rules and workflows. Generative AI expands these capabilities enabling users to interact with information using natural language, generate content, summarize complex data, and support decision-making. Agentic AI takes the next step. AI agents can be assigned a goal, determine the actions required, interact with authorized systems and data, execute multiple steps, evaluate results, and engage people when decisions are required.

Federal IT Is Moving Beyond Automation - Agentic AI is quickly moving from experimentation toward enterprise adoption. In February 2026, the National Institute of Standards and Technology (NIST) launched its **AI Agent Standards Initiative**, recognizing that AI agents capable of autonomous actions require standards that support secure operation and interoperability across the digital ecosystem. (NIST) The national security community is moving in the same direction. The June 2026 National Security Presidential Memorandum on AI directs the national security enterprise to accelerate AI adoption in

Continued on page 2



ActioNews®, the newsletter of ActioNet, Inc. is published to provide examples and applications of cutting edge IT topics and practices.

ActioNews® is published quarterly (March, June, September and December) as a service to its staff, customers, and potential customers.

ActioNews Staff

Lead Designer
Karen Tepera

Contributing Authors
Eric Chasteen
Sandra Montiel

ActioNet grants permission to educators and academic libraries to use ActioNews® for classroom purposes. There is no charge to these institutions provided they give credit to the author, ActioNews®, and ActioNet. All others must request permission at actionews@actionet.com.

ActioNet, Inc.
2600 Park Tower Drive
Suite 1000
Vienna, VA 22180
www.actionet.com
info@actionet.com

Copyright © 2026 by ActioNet, Inc.

**“Agentic AI
does not
replace the
Federal
modernization
journey-it
builds on it.”**

Advancing continued from page 1

mission areas where it can improve operational effectiveness, while emphasizing reliability, security, testing, interoperability, oversight, and accountability. (The White House)

Agentic Operations Build on the Modernization Journey - An AI agent operating inside a Federal enterprise needs more than a powerful model. It needs trusted data, secure access, APIs, identity and permissions, cloud infrastructure, workflows, cybersecurity controls, monitoring, auditability, and clearly defined human decision points.

Agentic AI does not replace the Federal modernization journey—it builds on it.

Through the Data Ingest and Collection for the Enterprise (DICE) solution, ActioNet applied cloud-native architectures, AWS EKS-based microservices, Infrastructure-as-Code (IaC), automated CI/CD pipelines, security controls, and automated data-quality checks for the US Department of Commerce. Capabilities have reduced system deployment time by 75 percent, while supporting 24/7 production operations and continuous security and compliance monitoring. Our Enterprise Data Lake (EDL) work extended that foundation through automated data migration, ETL and harmonization pipelines, role-based access, standards-based APIs, continuous monitoring, and FinOps. The result reduced computing infrastructure costs by 36 percent while maintaining 100 percent uptime for the EDL.

Automated Cybersecurity & Continuous Compliance at Dept. of State leveraging Splunk Enterprise, Cribl, Qmulos, Microsoft Defender, Oracle DBSAT, SCAP, compliance dashboards, & AI/ML pipelines.

From Automated Workflows to Intelligent Workflows - Consider a traditional IT service workflow, where automation can route an incident, notify the right support team, initiate an approval, provision a resource, or execute a predefined remediation. An AI-enabled environment can help analyze the incident, summarize relevant knowledge, recommend an action, and assist the technician.

An authorized agent could evaluate the request, gather information from multiple systems, identify the affected configuration items, review knowledge and prior incidents, execute approved diagnostic actions, coordinate supporting workflows, document the results, and escalate the issue when human judgment is required. Similar patterns can apply beyond IT service management—to cybersecurity, application development, data operations, cloud management, asset management, acquisition support, and mission business processes.

Governance Must Evolve With the Technology - This is a journey we discussed in a previous ActioNews article. Our *ActioNet AI Intelligent Capability Lifecycle™ (ICL)* treats AI as an evolving capability rather than a one-time technology implementation. It integrates program management, enterprise architecture, data strategy, Agile delivery, security, governance, operations, and continuous optimization. (ActioNet, Inc.)

ActioNet enabled Intelligent Enterprise Workflows for Federal customers at Commerce and State through managed services leveraging ServiceNow ITSM, ITOM, ITAM, workflows, KCS, automation, dashboards, & AI capabilities.

Agentic Operations reinforce the need for our lifecycle. As agents gain access to enterprise systems and execute increasingly complex tasks, organizations need to understand what the agent is authorized to do, what data it can access, what decisions require human approval, how its actions are logged, how performance is measured, and how the capability is continuously tested and improved.

NIST's new AI Agent Standards reflect these same aspects, including secure interaction with external systems, interoperability, identity, authorization, and trustworthy agent behavior. (NIST)

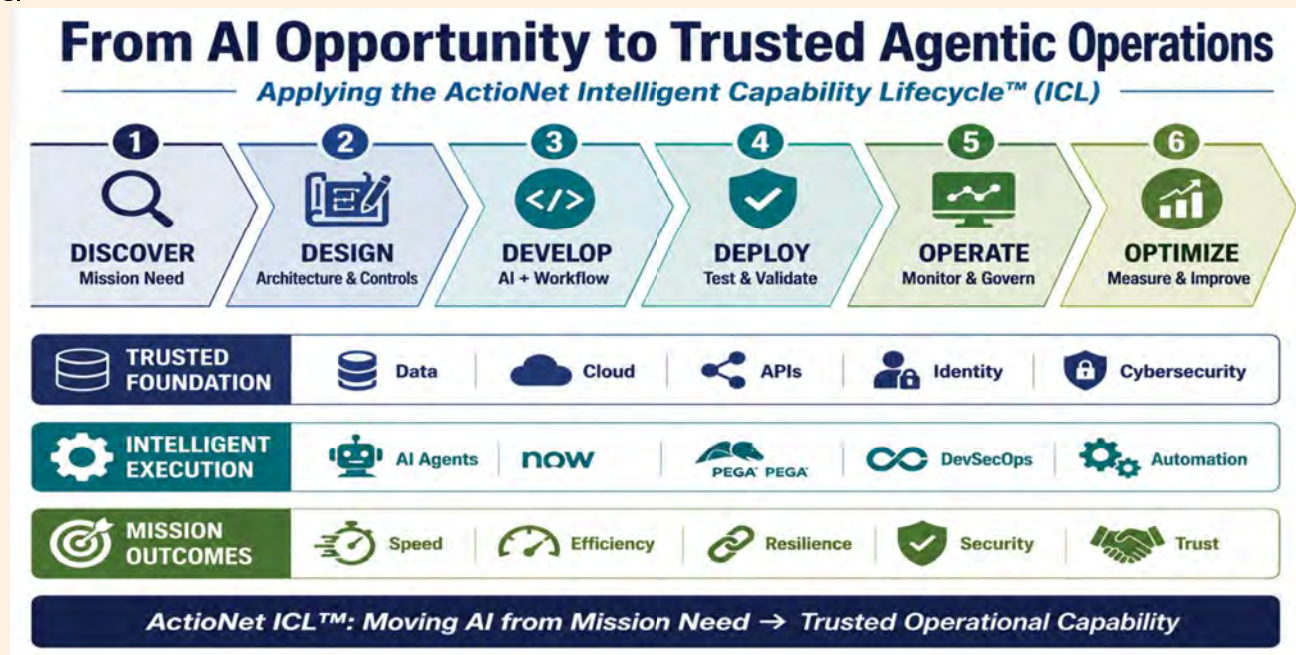
Turning Today's Operations Into Tomorrow's Agentic Enterprise - The path to Agentic Operations does not require agencies to replace the investments they have. It requires connecting them. Cloud platforms provide scalable compute and data services. APIs allow systems to exchange information and execute functions. ITSM and workflow platforms orchestrate business processes. DevSecOps and Infrastructure-as-Code automate deployment. Zero Trust controls access to systems and data. Observability provides insight into operational performance. Continuous compliance ensures security control remains effective.

ActioNet built data & cloud foundations for AI at Commerce leveraging AWS, EKS, Athena, RDS, Glue, Lambda, APIs, microservices, IaC, CI/CD, DevSecOps, & FinOps.

Continued on page 3

Advancing continued from page 2

The Next Step in the Journey - Agentic AI will not transform Federal operations simply because increasingly capable models become available. The real transformation occurs when agencies connect AI to trusted data, secure architectures, enterprise workflows, mission systems, and people—and manage those capabilities throughout their lifecycle.



Securing continued from page 4

The guidance recommends many of the same foundational security practices organizations already rely on, including data classification and access controls, encryption, trusted infrastructure, data provenance and ongoing risk assessments. The message is clear: AI security starts with data security. If the data used by an AI system cannot be trusted or adequately protected, neither can the results it produces.

We must also verify before we trust. AI can generate useful information quickly, but its output should not automatically be treated as accurate or authoritative. Just as we verify an unexpected email before clicking a link, we should consider the source, context, and accuracy of AI-generated information before relying on it, particularly when it is being used to support important business or security decisions.

As AI systems become more capable and autonomous, these habits become even more important. Cybersecurity awareness is no longer only about recognizing what may be trying to get into our systems. It is also about understanding what information we put into AI systems, what those systems can access, and how much authority we give them to act on our behalf.

Cybersecurity Awareness at ActioNet

AI awareness is part of cybersecurity awareness at ActioNet. As AI becomes more integrated into how we work, staying cyber aware means understanding not only the threats we face, but also how we use AI, what information we share with it, and when we should question or verify its output.

At ActioNet, we continue to promote a security-first culture through cybersecurity awareness training, phishing exercises, and established practices that help protect our systems and information. As our use of AI expands, those same cybersecurity fundamentals remain important. This includes protecting sensitive information, using trusted and approved technologies, controlling access to data, and continuously assessing risk. These principles align with joint CISA, NSA, FBI, and international guidance, which emphasizes protecting data throughout the AI lifecycle and maintaining security as AI systems are developed, deployed, and operated.

Cybersecurity awareness remains a shared responsibility, and at ActioNet, every action counts. Whether we are opening an email, entering information into an AI tool, reviewing AI-generated content, or allowing an AI system to take action, the decisions we make matter. Think before you click. Think before you prompt. Verify before you trust. By keeping security at the forefront of how we use technology, we all play a role in protecting ActioNet, our customers, and our mission as we work together to Secure the Next 250.

ActioNet is proud to support Cybersecurity Awareness Month and its mission to promote online safety and cybersecurity awareness. For more information about Cybersecurity Awareness Month 2026 and how to participate in a wide variety of activities, visit <https://www.cisa.gov/cybersecurity-awareness-month>.

- SBA Certified WOSB under NAICS 517111, 517121
- GWAC and IDIQ Contract Vehicles
 - GSA Alliant 2
 - GSAMAS
 - GSA OASIS Pool 1
 - CIO-SP3 SB/WOSB OTSB
 - DHAMHSGSP
 - DISA Encore III
 - ARMY ITES-3S
 - NAVY Seaport-NxG
 - FAA eFast
 - HHS SPARC
 - NRC GLINDA
 - SEC OneIT
- Past Performance on Large Contracts
 - DOE ITSS, \$12B
 - DOT COE, \$350M+
 - FAA ATO, \$300M+
 - CMS CIOCM, \$200M+
 - DOS CA DEDM, \$150M+
 - DISA CORENet, \$78M
- CMMC Level 2
- CSfC Trusted Integrator
- CMMI®-DEV Level 4
- CMMI®-SVC Level 4
- CMMI®-DATA Level 4
- CMMI®-SEC Level 4
- HDI Certified Support Center
- ISO 20000/27001/9001
- Approved Accounting System
- Approved EVM System
- Approved Purchasing System
- Approved Cost Estimating System



**“Think Before You Click,
Think Before You Prompt,
Verify Before You Trust.
With the use of AI,
consider what
information you are
sharing.”**

Securing the Next 250: Cybersecurity in the Age of AI

By Sandra Montiel, Cybersecurity Architect

October is Cybersecurity Awareness Month, an annual campaign led by the Cybersecurity and Infrastructure Security Agency (CISA) to raise awareness about cybersecurity and encourage safer online practices. This year's theme, “Securing the Next 250,” looks ahead to how we can build a safer and more secure digital future as the United States celebrates its 250th anniversary. Artificial intelligence has already transformed how we work, communicate, analyze information, and defend our systems. The challenge ahead is not simply adopting AI but ensuring that we use and secure it responsibly as its capabilities continue to advance.

In June 2026, Executive Order 14409, Promoting Advanced Artificial Intelligence Innovation and Security, reinforced the growing importance of securing AI by calling for stronger cyber defenses, expanded use of AI-enabled defensive capabilities, greater public-private collaboration, and protection against AI-enabled cybercrime.

This newsletter also explores agentic AI, which represents a shift from AI simply providing information to taking action and completing tasks on our behalf. Although this shift creates exciting possibilities, it also introduces new cybersecurity considerations. The more access and autonomy we give AI, the more important it becomes to protect the systems and data it can access and make sure the right safeguards are in place.



Think Before You Click. Think Before You Prompt. Verify Before You Trust.

For years, cybersecurity awareness has emphasized a familiar message: Think Before You Click. Every year, security awareness training reminds us to look closely at suspicious emails, links, and attachments before taking action. Those practices remain important, but as AI becomes more integrated into how we work, cybersecurity awareness must evolve with it.

Now we must also think before we prompt. The information entered into an AI system can be just as important as the information we choose to share through email, websites or other applications. Before entering information into an AI tool such as Copilot or ChatGPT, consider what information you are sharing, whether the tool is approved for that use, and whether the information is sensitive, proprietary or otherwise protected.

Protecting the data behind AI is becoming an increasingly important part of cybersecurity. Joint guidance from CISA, NSA, FBI and international partners emphasizes that data must be protected throughout the entire AI lifecycle, from development and testing through deployment and operation. The guidance identifies risks including compromised data supply chains, maliciously modified or “poisoned” data, and data drift, all of which can affect the accuracy, integrity and reliability of AI systems.

Continued on page 3