ActioNews

SPRING 2025
THE NEWSLETTER OF ACTIONET

CHAIRMAN'S NOTE

Dear Friends,

Spring is upon us and we are ready to tackle the challenges ahead. In this issue of ActioNews, we share how AI has been leveraged to transform the Department of Defense by leveraging Large Language Models (LLMs) and compute power. A new Executive Order issued in January 2025 is eliminating bureaucratic barriers and accelerating AI adoption.

We are also working closely with our Customers to streamline their implementations of the Risk Management Framework (RMF) by adopting a continuous model while reducing duplicative efforts and increasing visibility.

Our continued investments in people, process and technology strengthens team capabilities and fosters a culture of excellence, innovation, and long-term career growth.

Ashley W. Chen
Founder & CEO

IN THIS ISSUE

Turning **VISION** into **ACTION®**

How Large Language Models Are Reshaping the DoD

By Erick Mann, Chief Solution Architect

Over the past year, ActioNet has embraced AI as a transformative force— and with your help, we hosted pilot efforts for ChatGPT and Copilot, partnered with OpenAI, and established a corporate account that grants our users access to AI-powered bots. Our goal was clear: to orient our employees, build AI competence, and familiarize our teams with these powerful tools. We are achieving just that by integrating AI-driven automation into ServiceNow and offering ChatGPT bots to our employees to streamline their day-to-day activities and improve efficiency and innovation. As commercially available AI tools continue to reshape industries, a new frontier emerges; how Large Language Models (LLMs) and compute power are disrupting national security and the DoD.

The AI Disruption in Defense

For years, artificial intelligence in National Security was limited to classified environments, reliant on custom-built models running on specialized infrastructure. The Department of Defense (DoD) invested heavily in AI research, developing systems that required powerful, restricted computing resources. Fast Forward to the present day, and the rise of consumer-accessible AI has flipped that paradigm. Suddenly, the same tools once exclusive to government agencies are available to anyone with a high-end gaming PC and an internet connection.

Nowhere is this shift more apparent than in the rise of DeepSeek, an AI model that has made waves in the industry. When news broke that DeepSeek was running on NVIDIA's 4090 GPUs—the same hardware found in gaming rigs—shock waves spread through the tech world. Some claimed it was a breakthrough, a $6 million open-source project challenging billion-dollar AI firms like OpenAI and Google, but the truth was less revolutionary and more opportunistic. DeepSeek had simply stockpiled consumer-grade GPUs before the U.S. imposed trade restrictions, allowing it to scale rapidly while others scrambled for hardware.

This has left the defense sector grappling with a pressing question: if adversaries can build innovative AI with consumer hardware, how does the U.S. maintain its strategic edge? An executive order - REMOVING BARRIERS TO AMERICAN AI INNOVATION.

This executive order means that the U.S. government has recognized the role of commercial innovation, (in this case AI) plays in national security and economic growth. A new Executive Order issued in January 2025 is eliminating bureaucratic barriers and accelerating AI

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
Erick Mann
Sandra Montiel

> **“We can quickly get to the point of automating tasks, accelerating problem solving and helping customers achieve results faster than ever before.”**

Large Language Models continued from page 1

adoption, calling for:

- Revision of outdated AI policies that have slowed private sector development.
- Prioritization of AI in national security and economic strategy.
- Development of a Federal AI Action Plan to maintain U.S. leadership.

For ActioNet, this is an opportunity to be at the forefront of AI-driven government solutions. We are already prioritizing and investing in AI for briefings, automation, employee and customer self-service support and cybersecurity. All of these activities leverage Artificial Intelligence and are shaping the way federal agencies adopt and secure AI. Every time we provide over-the-shoulder support, guiding our customers in adopting AI into their daily operations, we are actively implementing the new executive order. These moments in our daily, weekly, and monthly reports to customers have accelerated fulfilling Mission Objectives and reduced redundancies.

ActioNet’s AI-Driven Mission

For ActioNet, our mission is not to simply follow AI trends, it is to lead, and that starts by arming our teams with AI tools that enhance expertise and expand capabilities. AI is no longer confined to elite research labs or DoD-backed initiatives—today, it must be accessible to every professional, not just data scientists and specialized teams. That is why we have empowered our employees with AI-powered tools like ChatGPT, not just as a convenience, but to lower the barrier to advanced problem solving. This includes briefings, In Progress Reviews (IPRs), financial reports, sifting through vast amounts of documentation to find key insights, and solving problems that customers have had for a long time but lacked the labor to do it. AI can make these processes faster and more efficient. Our goal is to create ready-made AI tools that reduce manual workloads and give employees more time to focus on high value work.

Many have become the go-to experts for tools like Power BI, streamlining analytics and decision making. AI is the natural next step. We can quickly get to the point of automating repetitive tasks, accelerating problem solving and helping customers achieve results faster than ever before. Whether we are summarizing massive reports in minutes or providing over-the-shoulder support on AI-driven insights, our growing expertise in AI is already making a difference.

Securing the Future with AI

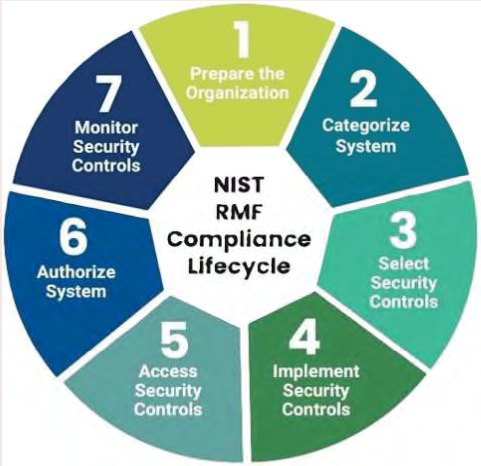
AI is more than just a tool. It is a strategic advantage. From optimizing workflows to protecting critical infrastructure, the responsible application of AI will define the next decade of innovation.

The AI landscape is changing rapidly, and the question is not whether AI will reshape national security—it already has.

Implementing Risk Management Framework at Mission Speed

By Sandra Montiel, Sr. Information System Security Officer

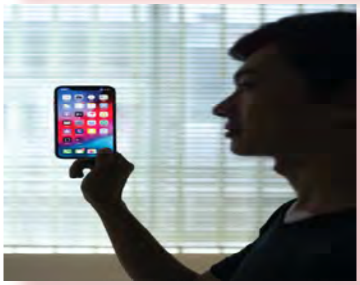
ActioNet helps agencies take the complexity out of cybersecurity compliance. We work alongside our customers to simplify the Risk Management Framework (RMF) process, bringing together automation, DevSecOps, and continuous compliance to reduce delays, minimize manual efforts, and keep mission-critical systems moving forward. Think of RMF as a routine health check for your IT systems—it helps you catch risks early, stay in compliance, and keep everything running securely and smoothly. Whether it's streamlining control assessments or enabling faster authorizations, our goal is simple--we help organizations stay secure without slowing down or disrupting the mission.



The traditional RMF process, while foundational to cybersecurity compliance, is increasingly misaligned with the pace of today's operational demands. Manual documentation, repetitive control validations, and delayed assessments continue to impede the timely deployment of mission-critical capabilities.

These challenges are compounded by:

> "Without real-time insights, decision makers are left in the dark - unable to assess risk accurately or respond proactively."



Lengthy Authorization Timelines:

Achieving an Authority to Operate (ATO) can take 12 to 18 months- sometimes even longer—due to sequential, manual workflows that require exhaustive documentation, multi-tiered reviews, and limited integration of security into the development lifecycle. It's like building a house and only calling the inspector after it's finished—when issues are found, everything must be torn down and rebuilt. Similarly, cybersecurity is often addressed after development is complete, causing rework and delays. A lack of standardization across systems and incomplete evidence for control implementation often cause delays during validation. This forces program offices into a reactive compliance posture, ultimately slowing down mission delivery.

Duplicative Compliance Work Across Systems:

Imagine having to prove the safety of the same firewall over and over—across every system—even though it was already validated in another project. That's what many organizations face today. Security controls are often revalidated across systems, even when those controls have already been approved within a shared infrastructure. Without leveraging inherited controls and reusable documentation, teams waste time, increase costs, and risk inconsistencies in how compliance requirements are interpreted.

Limited Visibility into System Security Posture:

You can't manage what you can't see. Many agencies still rely on point-in-time assessments, providing only static snapshots of security compliance. But in fast-paced, agile environments, systems change rapidly, configurations shift, and new vulnerabilities emerge every day. Without real-time insights, decision-makers are left in the dark—unable to assess risk accurately or respond proactively. This limits Authorizing Officials' (AOs) ability to make timely, risk-informed decisions.

Continued on page 4

ActioNews

- SBA Certified WOSB under NAICS 517111, 517121
- GWAC and IDIQ Contract Vehicles
  - GSA Alliant 2
  - GSA MAS
  - GSA OASIS Pool 1
  - CIO-SP3 SB/WOSB OTSB
  - DHA MHS GSP
  - DISA Encore III
  - ARMY ITES-3S
  - NAVY Seaport-NxG
  - FAA eFast
  - HHS SPARC
  - NRC GLINDA
  - SEC OneIT
- Past Performance on Large Contracts
  - DOE ITSS, $1.2B
  - DOT COE, $350M+
  - FAA ATO, $300M+
  - CMS CICDIM, $200M+
  - DOS CA DEDM, $150M+
  - DISA CORENet, $78M
- CMMI®-DEV V2.0 ML 4 with SAM
- CMMI®-SVC V2.0 ML 4 with SAM
- HDI Certified Support Center
- ISO 20000/27001/9001
- Approved Accounting System
- Approved EVM System
- Approved Purchasing System
- Approved Cost Estimating System

TOP
WORK
PLACES
2014-2024

ActioNet, Inc.
2600 Park Tower Drive
Suite 1000
Vienna, VA 22180
PHONE 703-204-0090
FAX 703-204-4782
info@actionet.com
www.actionet.com

ActioNet

Implementing RMF with Mission Speed

continued from page 3

Overburdened Security Teams and Labor-Intensive Processes:

Managing RMF compliance often requires time-consuming administrative tasks—compiling evidence, maintaining documentation, tracking Plan of Action and Milestones (POA&Ms), and supporting control assessments—all on top of daily security operations. As system portfolios grow, the absence of automation and streamlined workflows only adds to the burden, increasing the risk of delays, staff burnout, and gaps in security coverage.

In environments where agility and resilience are imperative, there is a clear need to shift from static, one-time authorization models toward a more continuous, integrated, and automated RMF approach.

How ActioNet Simplifies RMF and Accelerates Outcomes

✓ ActioNet supports agencies in streamlining and improving their RMF processes by moving away from traditional 3-year ATO cycles and embracing continuous compliance supported by automation. Our approach reduces complexity, minimizes manual overhead, and aligns cybersecurity efforts with mission delivery. **We don't just comply—we operationalize compliance to support mission success!**

Security Control Inheritance and Platform-Level Reuse

✓ We reduce duplicative efforts by identifying and documenting common controls that can be inherited across multiple systems. By leveraging enterprise or platform-level security artifacts, our teams enable reuse of pre-approved documentation, accelerating compliance activities while ensuring consistency across the enterprise.

Integrated DevSecOps and CI/CD Pipelines

✓ ActioNet embeds RMF compliance into the system development lifecycle, enabling continuous security integration through DevSecOps practices. We support system owners in transitioning to continuous ATO (cATO) environments, allowing secure and agile deployments through automated control validations within software pipelines.

Compliance Automation and Dashboard-Driven Monitoring

✓ The Enterprise Mission Assurance Support Service (eMASS) and the Cyber Security Assessment and Management (CSAM) system are government-mandated compliance management platforms used to support RMF activities across the Department of Defense (DoD) and other federal agencies. While these systems are essential for tracking system compliance and managing security control documentation, they often present challenges—such as limited native automation, manual data entry requirements, and fragmented reporting capabilities. These limitations can slow down the compliance process and create unnecessary administrative burden for security teams. ActioNet helps automate control assessments, POA&M management, and continuous compliance tracking through integration with tools such as SteelCloud for STIG automation, eMASSter for POA&M generation and automated control data population and reporting in eMASS, and Axonius for asset inventory and control gap analysis. We also develop custom dashboards using Power BI or Tableau to aggregate data from eMASS or CSAM to deliver real-time visibility to Authorizing Officials (AOs) and mission stakeholders.

Workforce Readiness and Continuous Training

✓ ActioNet's professional development and benefits program reflects our deep commitment to building a skilled, mission-ready workforce. We provide targeted training, cross-functional mentorship, and support for industry-recognized certifications—empowering our employees to grow their careers while contributing to high-impact, mission-driven work. Our investment in people not only strengthens team capability but also fosters a culture of excellence, innovation, and long-term career growth.