Spectro Cloud
GOVERNMENT

Accelerating ATO to Meet the Military's Need for Capability at the Tactical Edge

Overcome the bottlenecks in the government's authorization model while securing cloud architectures at the tactical edge, key to keeping pace with today's modern, AI-driven battlespace.

A SPECTRO CLOUD WHITE PAPER

PUBLISHED BY AFCEA INTERNATIONAL

Executive summary

The modern battlefield operates at machine speed—but the governmental acquisition processes that enable it often do not.

As the Department of War pushes AI, advanced analytics, and software-defined capabilities to the tactical edge, the Authority to Operate (ATO) process remains a critical bottleneck. Designed for centralized, connected environments, today's authorization model struggles to keep pace with forward-deployed, disconnected, and contested operations, delaying mission-critical capabilities while adversaries move faster.

There needs to be a new way to accelerate ATO so the U.S. can respond quicker to threats, and deliver capabilities faster as dynamics on the battlefield change.

Spectro Cloud Palette VerteX combines hardware and software from trusted partners to accelerate mission/AI-ready edge deployments. Expert at extending secure cloud architectures to the tactical edge, Spectro Cloud equips team leads with a pre-validated, zero-trust compute foundation that includes all necessary controls to meet NIST 800–53 compliance requirements, eliminating the need to rebuild or revalidate security from scratch. This approach streamlines the software ATO process, cutting months from deployment timelines while ensuring consistent cybersecurity posture across cloud and edge environments. Agencies can rapidly field AI and autonomous systems in disconnected, contested, or classified environments — improving decision speed, resilience and mission effectiveness without compromising compliance or security.

Securing the tactical edge with repeatable infrastructure for accelerated ATO

The latest advances in software, particularly for machine learning (ML) and artificial intelligence (AI), are pivotal to shaping the modern battlefield, where adapting to threats demands actionable insights. Unfortunately, the Pentagon's traditional software approval process has impeded how quickly software advances reach the front lines.

The DOD requires companies to complete the process, known as the Authority to Operate (ATO), before software systems can run within a DOD environment. Specifically, the ATO process verifies that information systems meet stringent security and privacy standards before deploying on a network. It focuses on documenting security controls, scanning for vulnerabilities, performing risk assessments, and ensuring compliance with frameworks like NIST Risk Management Framework (RMF).

An authorization & compliance burden

For over a decade, ATO has guided the Pentagon's acquisition process, helping identify and manage cyber risks on DOD networks. But both government and industry experts acknowledge that the system is broken, hindering U.S. forces from acquiring the latest capabilities to anticipate and respond to adversaries.

In a June 2025 interview with *DefenseScoop*, Acting Department of Defense Chief Information Officer Katie Arrington called both ATO and its sister process, the RMF, "old school" and not reflective of the modern technologies needed by the Pentagon.

Mark Perry, director of public sector growth for Spectro Cloud, a leading Kubernetes enterprise software firm, agrees. "You're looking at 12 to 24–month delay. [The ATO's long approval time] is preventing these capabilities from being fielded by our warfighters, and our adversaries don't have the same limitations," he says.

The ATO challenge is particularly stark as modern military operations move increasingly to the tactical edge. That's because ATO by design requires applying static, compliance-heavy security frameworks to dynamic, physically vulnerable and disconnected environments.

The process is hindered by the need for onsite, low-latency performance in contested areas, making traditional, centralized, manual security reviews insufficient. Case in point: tactical systems cannot rely on continuous reachback to cloud services for authentication or security monitoring. They operate autonomously. In addition, the ATO process often assumes a static system, while edge solutions require rapid, continuous updates (DevSecOps) to meet changing mission needs. Finally, edge hardware often has limited power, computing and bandwidth, making it difficult to run heavy security agents.

The push to enable decision-making in forward-deployed, disconnected and contested environments has resulted in a convergence of two challenges – getting the formal "go-ahead" to operate from an authorization and cybersecurity/regulatory standpoint and deploying and sustaining tactical edge systems.

At the tactical edge, military operators can't rely on the same assumptions as a data center or enterprise cloud environment. Systems must be resilient, secure, compliant and increasingly, semi-autonomous and able to operate without continuous connectivity.

If defense suppliers don't get the ATO and the systems designed for edge right, they risk delays, mission failure or security exposure.

The tactical edge bottleneck

Operators find themselves in a "tactical edge bottleneck," where they face denied, disrupted DDIL environments when rapid-real-time decision-making is needed most.

- ### SWaP constraints

  Too often, this bottleneck is marked by size, weight, and power (SWaP) constraints, ruggedization needs and environmental (temperature, shock, vibration) demands. These constraints affect how a system will pass DOD security/certification requirements. For example, users may have limited ability to patch/upgrade or may face less compute capacity or special power constraints.

- ### More friction

  In addition, every patch, upgrade, or new container requires revalidation, creating friction because mission teams cannot deploy or update applications quickly enough to respond to evolving threats or data needs.

- ### Greater complexity

  In a tactical-edge context, operators must deal with extra complexities: mobile/disconnected nodes, ruggedized hardware, variable connectivity and higher threat environments, which all translate to more risk. This means justification, risk acceptance and controls may be more complex.

- ### Unreliable connectivity

  There are also connectivity and networking challenges unique to the edge environment. For one, edge nodes may be disconnected, intermittently connected, or face jamming or other hostile interference.

The backhaul and lifecycle challenge

According to Ditto, an end-to-end synching platform provider, users also face a "backhaul" problem; namely, how to get critical data/sync back to enterprise systems or headquarters, manage updates, or perform centralized monitoring when connectivity is constrained.

For ATO, this means that monitoring, auditing, vulnerability scanning and patch management must work under constrained or offline conditions. Without reliable connectivity, users may struggle to meet certification/control requirements, especially considering that traditional systems aren't built for disconnected operations. Furthermore, if connectivity is intermittent, users will need alternative mechanisms (local logging, delayed sync).

Then there's the need to oversee device lifecycle management: how long will edge devices stay deployed, in what state, and will the ATO remain valid if hardware/software evolve? The authorization must cover change management.

Edge: A new level of security threat

When it comes to security, the tactical edge is higher risk: devices can be physically captured, communications intercepted, and nodes compromised, finds Maris, an AI edge video and analytics technologies provider. Thus, security controls must anticipate physical compromise, tampering, loss of connectivity and fallback modes. Hardening devices, encryption and tamper-proofing become more important, and harder, adds Booz Allen in a four-part series examining obstacles to the military's adoption of edge computing.

The authorization process must evaluate these threat vectors and ensure the system's risk posture is acceptable; in contested terrain, the bar is higher.

Integration, supply chain challenges

The tactical edge often requires firms to integrate with legacy platforms, older systems and heterogeneous suppliers. Edge devices could range from vehicles and drones to radios and sensors, all having limited self-update capacity.

Even the supply chain for hardware/software in austere settings is more challenging: the environment demands more rugged parts, trusted vendors and fewer refresh cycles. For ATO, companies must demonstrate supply-chain risk management as well as interoperability because users may need to operate with coalition/partner systems, mesh networks and varied devices.

Embracing continuous ATO

Continuous ATO, or cATO, which uses DevSecOps practices for software development, is helping address these challenges unique to the tactical edge. This new DOD process streamlines ATO to accelerate delivery of the most advanced secure software to warfighters. The relatively new Pentagon process moves away from document-based, point-in-time technical security assessments to continuous monitoring, active defense and automated assessments to maintain security and compliance in near real time.

Spectro Cloud: Answering the secure edge & ATO challenge

Spectro Cloud has seen the challenges and urgency of moving capability to the tactical edge through its work with government end users. It understands the software regulatory and certification landscape. Working with partners, Spectro Cloud offers a way to simplify and accelerate the process, offering an "ATO-in-a-box" capability through its Palette VerteX platform, a secure, compliant and scalable Kubernetes management platform designed for government and regulated industries.

ATO in a box

"Our concept is that you can grab already-authorized layers of software and then stack them together," explains Scherer. "The biggest problem we're looking to solve with our concept of 'ATO in a box' is the physical box by giving our customers that hardware that is pre-validated. It has multiple layers of encryption; it allows the storing of classified data; it's ruggedized; and it can be rapidly fielded."

Palette VerteX streamlines the Authority to Operate process at the tactical edge by reducing risk and uncertainty. Its pre-validated, immutable software stacks give program offices a consistent baseline that can be reused across missions. It also includes built-in security features — from trusted boot and Federal Information Processing Standards (FIPS)-validated encryption to Software Bill of Materials scanning and tamper-proof logging — providing the documentation and evidence RMF assessors need.

DOD-aligned for faster authorizations

Because Palette VerteX can operate fully offline while maintaining audit integrity, and because it aligns with DoD initiatives like Platform One and TradeWinds, the platform helps field teams achieve faster, repeatable authorizations instead of starting from scratch for each mission.

"Users can use the same piece of equipment to do multiple mission sets or change the mission sets," Scherer says.

> "Our Palette VerteX software platform doesn't magically 'grant' an ATO and solve the secure edge speed issue for teams. What it does is make the ATO process faster, easier and less risky by giving the Authorizing Official a system that's predictable, well-documented and continuously compliant. It effectively shrinks the unknowns that usually slow down the RMF process."
>
> —Mark Perry, Director of Public Sector Growth, Spectro Cloud

Six recommendations to be cATO-ready

Spectro Cloud offers six ways to be cATO-ready as the Pentagon accelerates modernization:

1. Use modular, open architectures to reduce integration risk and make future authorization updates easier (one of the obstacles is too much uniqueness per device/system).
2. Ensure your hardware and software for edge deployments have ruggedized/security-centric capabilities (tamper detection, hardened OS, minimal footprint, power/back-up resilience).
3. Define clear procedures for offline/disconnected operation: how does the system monitor security, log events, handle updates, synchronize when connectivity returns.
4. Plan for supply chain and device lifecycle: who will update firmware, patch devices, replace hardware, and how will this impact your authorization posture.
5. Map the risk model: evaluate physical, cyber, connectivity risks in the edge scenario and ensure the Authorizing Official (or equivalent) is comfortable with residual risk.
6. Engage early with accreditation/certification stakeholders so the edge-specific constraints are understood rather than treated as exceptions.

Strong demand seen as DOD modernizes C2 infrastructure

Spectro Cloud VerteX meets multiple use cases, from intelligence, surveillance and reconnaissance (ISR) and command and control (C2) to humanitarian assistance and coalition interoperability — anywhere rapid, reliable and compliant compute is needed.

"We're seeing command-and-control terminals being modernized throughout the DoD," says Scherer, citing the Army contract with Anduril and Palantir for next-generation C2. Similarly, there is a broad effort to modernize the entire Nuclear Command, Control and Communication (NC3) architecture.

"As we start to modernize our strategic deterrence, we're seeing more connectivity and ruggedized kits being put out there, which is creating more demand for a solution like this in the marketplace," Scherer adds.

To date, Spectro Cloud has fielded its platform broadly, including to the U.S. Air Force and to a SAIC lab, with plans to deploy it to other U.S. military branches. For SAIC, Spectro Cloud has demonstrated the ability to develop and deploy the software from the cloud to a disconnected edge device.

The boxes below show two different use cases for VerteX.

USE CASE 1	USE CASE 2
A forward-deployed unit receives a SNUC rugged edge node preloaded with Spectro Cloud VerteX. Within minutes:	
• A secure FIPS-validated Kubernetes cluster is operational. • Messaging and C2 applications are deployed. • When the network drops, the system keeps running autonomously. • Once connectivity returns, VerteX automatically syncs compliance and logs with higher command. • The result: mission-ready infrastructure deployed in minutes — not months.	• A secure Kubernetes cluster is operational. • AI models for image recognition and signal analysis are deployed alongside tactical messaging apps. • The system performs on-device inference, detecting objects or threats in sensor feeds. • Even if disconnected, the cluster continues to process data and feed alerts to command nodes. • When connectivity resumes, VerteX automatically syncs mission logs, model updates, and compliance status to higher headquarters. • The result: real-time, AI-powered situational awareness, continuously compliant and operational even in disconnected conditions.

Conclusion

Spectro Cloud Palette VerteX offers the right "in-a-box" solution to accelerate mission/AI-ready edge deployments by extending secure cloud architectures to the tactical edge.

DOD users can leverage a pre-validated, zero-trust compute foundation that includes all necessary controls to meet NIST 800–53 compliance requirements, eliminating the need to rebuild or revalidate security from scratch.

This approach streamlines the software ATO process, cutting months from deployment timelines, while ensuring consistent cybersecurity posture across cloud and edge environments.

Agencies can rapidly field AI and autonomous systems in disconnected, contested or classified environments — improving decision speed, resilience and mission effectiveness without compromising compliance or security.

To learn more about Spectro Cloud's Palette VerteX offering for government, visit SpectroCloud.com:

- **Product collateral –** https://www.spectrocloud.com/resources/collateral/palette-vertex-accreditations-pdf
- **News release –** https://www.spectrocloud.com/news/spectro-cloud-announces-palette-vertex-for-government
- **Book a demo –** https://www.spectrocloud.com/get-started

Spectro Cloud
GOVERNMENT

About Spectro Cloud

Turn the chaos of Kubernetes into effortless control, wherever your mission takes you

Spectro Cloud Government delivers the power of Kubernetes to missions where security, compliance and resilience are critical.

Through our award-winning Palette VerteX platform, purpose-built for regulated organizations, we give public-sector teams the power to design, deploy and manage Kubernetes at scale. Palette VerteX provides a consistent, governance-approved platform with FIPS 140–3 cryptography that functions across every domain, from the classified data center, hyperscaler gov clouds and air-gapped sites to the far tactical edge.

Palette VerteX is already trusted by teams across the Army, Navy and Air Force, and is 'Awardable' on both the Platform1 and CDAO Tradewinds solution marketplaces. Industry analysts GigaOm position us as a "Leader" and "Outperformer" in their 2025 Radars for both Managed Kubernetes and Kubernetes for Edge Computing. Our certifications with standards like ISO 27001 and SOC 2 Type 2 evidence of our continuous, audited controls.

Whether you're powering AI-driven situational awareness for war-fighters or digital services for millions of citizens, Spectro Cloud Government with Palette VerteX delivers secure, compliant and scalable Kubernetes — so your agency can focus on mission outcomes, not infrastructure.

Learn more about Spectro Cloud and the Palette platform at spectrocloud.com.