Cav Expands U.S. Coast Guard Deployment Fleetwide as Federal Agencies Prioritize Continuous Cyber Assurance

WASHINGTON — CAV, the continuous cyber assurance company trusted by leading government agencies and Fortune 500 enterprises, today announced a period of record growth, capped by a fleetwide expansion of its deployment with the U.S. Coast Guard (USCG). Annual recurring revenue has grown more than 500% year over year, and the company is on pace to be both cash-flow and EBITDA positive for fiscal year 2027.

Cav’s growth reflects an operational shift happening across high-reliability organizations (HROs): how they handle cyber compliance. Today, cybersecurity is the last major regulated risk area still relying on periodic, manual, sample-based audits. Other risk areas such as market risk, anti-money-laundering, and trade surveillance were automated more than a decade ago. This outdated approach not only fails to protect against modern cyberthreats, it also costs businesses and government agencies tens of millions of dollars every year.

As a result, federal agencies are increasingly moving toward continuous cyber assurance adoption. The Cav Compliance OS™ platform is purpose-built to meet the rigorous demands of these mission-critical systems with speed and accuracy.

U.S. Coast Guard: From Two Pilots to Fleetwide Standard

Cav's expansion with the USCG follows two successful pilots: the first addressed an enterprise IT use case and the other targeted operational technology (OT) aboard USCGC Storis, a commercial vessel recently acquired by the Coast Guard for its expanding icebreaker fleet. In that OT pilot, Cav compressed the authorization timeline by 90%, from years to weeks. On the strength of those results, the Coast Guard expanded Cav fleetwide, making Compliance OS its cyber assurance platform of choice.

"USCG selected Cav to operate across the entire fleet – ships, drones, shore installations and air platforms – because we are the only continuous compliance platform to span classified and air-gapped environments in production. Unclassified through Top Secret, we understand firsthand that systems must be mission-ready at all times," said Ish Boyle, CEO of Cav. "Over the past year, geopolitical conflict, particularly at sea, has heightened awareness of the importance of combat readiness. Cav makes mission assurance real-time instead of point-in-time. This capability is now available to any federal agency, defense contractor, or critical infrastructure operator still treating compliance as something done periodically instead of continuously."

A Year of Compounding Milestones

The Coast Guard expansion is one of several milestones over the past 12 months, including:

- **Compliance OS launch:** Cav introduced its agentic AI-powered platform delivering audit acceleration and continuous cyber controls monitoring across cloud, on-premises and air-gapped environments.

- **FedRAMP High Authorization:** The company achieved this status in partnership with the U.S. Department of Health and Human Services, streamlining procurement for NIST 800-53-based continuous compliance across the Department of Defense and civilian agencies.
- **Customer traction:** 14 new contracts were executed across U.S. government and defense technology customers, including four new contracts closed in June and July 2026. Customers include the U.S. Air Force, U.S. Coast Guard, U.S. Navy, U.S. Space Force, the Department of Health & Human Services, BNP Paribas and Fiserv, among others.
- **Team Growth, Leadership + Recognition:** Cav's headcount grew to 27, more than 50% year over year. Bobby Tuohy was named Chief Product Officer and Cav was named to the 2026 Inc. 5000 list of the fastest-growing private companies in America.

The Market Behind the Momentum

The regulatory direction is now unambiguous: continuous monitoring as the baseline expectation, evidence-backed assurance in place of attestation, and continuous control assessment in place of periodic audit. Continuous Controls Monitoring has emerged as a formal Gartner category, defined in the 2026 Gartner Market Guide for DevOps Continuous Compliance Automation Tools, and the market is splitting into two value chains, including legacy workflow-driven compliance automation and agentic AI-native continuous assurance. Cav is the AI-native entrant defining the second value chain.

he global governance, risk and compliance (GRC) market is roughly $60 billion in 2026, projected to exceed $150 billion by 2034 with North America driving more than 35% of that spend. Two near-term segments anchor demand for Cav's technology:

- The first is U.S. federal compliance and authorization automation, part of the roughly $20 billion in annual federal cybersecurity spending. FedRAMP 20x, NIST RMF revisions, and continuous-authorization mandates are concentrating the budget here.
- The second is financial services, where the FFIEC Cybersecurity Assessment Tool's retirement and the shift to the Cyber Risk Institute Profile open a defined buying window in 2026–2027, against roughly $61 billion in annual global compliance-technology spend.

"Compliance is no longer a department within HROs, it is part of the core operating model," said Boyle. "Our growth this year is a reflection of government agencies, enterprises and critical infrastructure providers embracing agentic technology to transform their most labor-intensive operations. From inside data centers to connected edges on devices and platforms, Cav is enabling HROs to control the present and protect the future."

In recognition of the company's continued business momentum, Cav was recently named to the Inc. 5000, a ranking of high growth, privately held, for-profit and independent companies based in the United States that have demonstrated ability to generate revenue and measurably scale.

From Cav, 29 Sept. 2026