Mobilicom Launches Secured Autonomy™ Framework: A Common Structure for Cybersecurity in Autonomous Systems

Introduces a unified cybersecurity framework and technical primer to help secure autonomous drones and robotics across global operations

WASHINGTON, DC, UNITED STATES, October 13, 2025 /EINPresswire.com/ -- Mobilicom Ltd., a provider of cybersecurity and robust solutions for drones and robotics, today announced the Secured Autonomy™ Framework at the Association of the United States Army (AUSA) Annual Meeting & Exposition in Washington, D.C. The framework gives the autonomy industry a shared structure for describing, designing, and delivering cybersecurity across diverse systems. It organizes protection into three clear pillars that address distinct attack surfaces and enable consistent evaluation and interoperability across partners, platforms, and technologies.

> The Secured Autonomy Framework and book give the industry a clear path to design, measure, and validate cybersecurity for autonomous systems."
>
> *Oren Elkayam, CEO and Co-Founder*

Mobilicom will present the Secured Autonomy Framework during a detailed briefing on Tuesday, October 14, from 11:30 a.m. to 12:30 p.m. in Room 206A. The session will show how a structured approach to cybersecurity can accelerate secure adoption across defense, commercial, and public safety applications. Attendees will receive early-release copies of Secured Autonomy: A Cybersecurity Primer for Drones and Robotics.

Addressing the Industry Gap

Autonomous systems are expanding faster than the cybersecurity models that protect them. Manufacturers, operators, and regulators often assess risk with different criteria, which slows collaboration and complicates compliance. The Secured Autonomy Framework addresses this gap through three interdependent pillars. Secured Autonomous Platforms focus on onboard protection, safeguarding processors, firmware, and mission software at the host, network, and application layers. Secured Fleets provide coordinated protection, detecting and preventing systemic vulnerabilities across connected systems through update integrity, segmentation, and supply chain controls. Secured Communications protect control, telemetry, and payload links from interference, intrusion, and electronic warfare. Together, these pillars provide end-to-end

protection from platform core to fleet coordination to external communications.

Rising Expectations

Cybersecurity expectations for autonomous systems are increasing worldwide. Across defense, commercial, and public sectors, stakeholders are moving from voluntary guidelines to defined requirements. The Secured Autonomy Framework offers a reference model that helps teams align design, procurement, and compliance practices as standards evolve.

Demonstrating the Framework Through Partnership

Mobilicom is applying the framework through partnerships and integrated solutions. At AUSA, the company is demonstrating mission computing platforms including the SA Compute PRO-AT, developed with Aitech, and the SA Compute PRO-AR, developed with ARK Electronics. Both combine AI-driven mission computing with continuous onboard protection through Mobilicom's OS3 cybersecurity software. These collaborations reduce integration complexity for manufacturers and give operators platforms that meet stringent security needs without sacrificing performance or mission adaptability.

Comprehensive Technical Documentation

Secured Autonomy: A Cybersecurity Primer for Drones and Robotics documents the framework in depth. To Mobilicom's knowledge, it is the industry's first dedicated technical reference focused on cybersecurity for autonomous drones and robotics. The book provides threat models, prevention and mitigation strategies, and design checklists that engineers, operators, and procurement officials can use to evaluate security at every layer. It draws from more than fifteen years of real-world experience securing autonomous systems in sixteen countries. The early-release edition is available at AUSA, with ebook reservations open at mobilicom.com/securing-autonomy-book.

Open Framework for Industry Adoption

The framework is offered as an open industry reference. Mobilicom invites manufacturers, integrators, and standards bodies to adopt the three-pillar structure when evaluating cybersecurity requirements, designing system architectures, and developing procurement criteria. Organizations using the framework are encouraged to cite: "Secured Autonomy: A Cybersecurity Primer for Drones and Robotics (Mobilicom, 2025)."

Mobilicom's framework is designed to strengthen collaboration and support the evolution of standards. Building on participation in AUVSI's Trusted Cyber initiative and Blue UAS certification, Mobilicom aims to contribute operational insights to organizations working to align cybersecurity practices with real-world conditions and to advance practical, scalable standards across defense and commercial programs.

"When engineers, operators, and regulators work from a shared cybersecurity structure, the entire industry benefits," said Oren Elkayam, CEO of Mobilicom. "The Secured Autonomy Framework provides that structure. It helps teams design protection that is measurable,

interoperable, and adaptable to new threats and missions. That is how we advance autonomy safely and with confidence.”

About Mobilicom
Mobilicom is a leading provider of cybersecure robust solutions for the rapidly growing defense and commercial drones and robotics market. Mobilicom's large portfolio of field-proven technologies includes cybersecurity, software, hardware, and professional services that power, connect, guide, and secure drones and robotics. Through deployments across the globe with over 50 customers, including the world's largest drone manufacturers, Mobilicom's end-to-end solutions are used in mission-critical functions.

Anthony Miller
Mobilicom
anthony.miller@mobilicom.com
Visit us on social media:
LinkedIn
