

FOR IMMEDIATE RELEASE

Contact: **Faye Francy**
Executive Director, Auto-ISAC
fayefrancy@automotiveisac.com
703-861-5417

Auto-ISAC's Membership Adds Four Cybersecurity Companies
Advancing the Cybersecurity of the Connected Vehicle

Washington, DC – October 9, 2019 – [The Automotive Information Sharing and Analysis Center](#) (Auto-ISAC) welcomes two members, [TuSimple](#) and [Yamaha Motor Group](#) and two strategic partners, [ArmorText](#) and [Celerium](#).

The inclusion of these four companies increases the strength of the Auto-ISAC's position as the voice of the global auto cybersecurity information sharing community as it works to prevent cyber threats to the connected vehicle.

The Auto-ISAC was formed by automakers in 2015 to promote collaboration between suppliers, commercial vehicle companies and automobile manufacturers around vehicle cybersecurity issues. Additionally, the Auto-ISAC has a strategic partner program that brings great value to our membership collaborating with innovators who support learning and sharing tools and techniques in managing the emerging complexity of automotive cybersecurity.

"ArmorText, Celerium, TuSimple and Yamaha Motor Group all play critical roles in building the resiliency of our connected vehicle ecosystem, and their contribution to the Auto-ISAC is key to our industry's success," said Jeff Massimilla of General Motors, who serves as the Auto-ISAC's Chairman. "Collectively, these companies will contribute valuable information to drive the industry's proactive work to incorporate strong security measures into every phase of the vehicle lifecycle."

The Auto-ISAC operates as a central hub to share and analyze intelligence about emerging cybersecurity risks. The focus of the Auto-ISAC is to foster global collaboration for mitigating the risks of a cyber-attack and to create a safe, efficient, secure and resilient global connected vehicle ecosystem.

Geoff Wood of Harman and chairman of the organization's Affiliate Advisory Board, which represents non-OEM members said, "We all play a key role in the cybersecurity of connected vehicles. Sharing and analyzing cyber risk information benefits everyone and it is an important step welcoming these companies to contribute to our intelligence gathering actions."

A key action by the Auto-ISAC is the publishing of the automotive cybersecurity best practice guides that cover organizational and technical aspects of vehicle cybersecurity. Currently, six guides are available to the public: awareness and training; collaboration and engagement; governance; incident response; risk assessment and management; and, threat detection, monitoring and analysis.

The Auto-ISAC has global representation. Its members represent more than 99 percent of light-duty vehicles on the road in North America. Members also include heavy-duty vehicles, commercial fleets and carriers and suppliers. Its annual Summit is scheduled for October 23-24, 2019 and hosted by Toyota in Plano, TX. To register and become a sponsor of the Summit, please visit <https://www.automotiveisac.com/auto-isac-summit/> and follow us @autoisac.

#

For editors only:

ArmorText is the creator of ArmorText Secure Teams, a best-in-class collaboration (messaging, file sharing, voice, video, and screen sharing) platform built to meet the specific needs of critical infrastructure providers and regulated industries. ArmorText employs end-to-end encryption and Trust Relationships for secure information sharing, to provide a platform that delivers unrivaled functionality, governance, and information lifecycle controls.

ArmorText is currently working with automotive suppliers and manufacturers to secure research and development initiatives, existing intellectual property and sensitive communications. ArmorText is also providing education and awareness training to Auto-ISAC members on defenses that should be employed to stave off emerging threats to the automotive industry's customers, workforce, and profits.

Media Contact: John Villanueva, VP, Strategy, Marketing and Business Development
Mobile: (202) 644-8777
Email: john@armortext.com

TuSimple is developing the world's best autonomous driving solution for the long-hall trucking industry. They're committed to improving safety, increasing efficiency and decreasing operating costs through the implementation of self-driving technologies to heavy duty trucks. Today TuSimple is the only company capable of transporting freight from depot-to-depot autonomously on both highways and surface streets.

Media Contact: Stacy Morris
Phone: 310.415.9188
Email: stacy.morris@tusimple.ai

YAMAHA MOTOR Group is taking measures covering both tangible and intangible aspects of cybersecurity to increase protection against external attacks, to detect an attack at an early stage, and to minimize the damage in the event an attack were to occur.

Media Contact: Naoto Horie
Phone : +81-3-5220-7211
Email : horien@yamaha-motor.co.jp

Celerium provides the Cyber Defense Network (CDN) for Supply Chains. CDN helps improve the cybersecurity posture for supply chains of automotive OEMs to mitigate business impacts such as compromised and delayed products. CDN solutions for supply chains include informational solutions to build awareness and to mobilize OEM suppliers as well as cyber threat sharing solutions. Celerium currently provides Auto-ISAC with secure information-sharing solutions for collaboration among Auto-ISAC Members.

Media Contact: Lyndsi Stevens

Mobile: (850) 582-5351

Email: lstevens@celerium.com