

Commercial Vehicles to Join Auto-ISAC

Enhance Cybersecurity Protection of Today's Connected Vehicles

NEWS PROVIDED BY

Automotive Information Sharing and Analysis Center (Auto-ISAC) →

Jan 25, 2017, 15:39 ET

WASHINGTON, Jan. 25, 2017 /PRNewswire-USNewswire/ -- The Automotive Information Sharing and Analysis Center (Auto-ISAC) today announced it would develop criteria for the inclusion of the commercial vehicle segment in its membership.

Auto-ISAC was formed by light-duty vehicle OEMs in late 2015, and extended membership to light-duty vehicle suppliers in early 2016. Building upon the success of this collaboration, the beginning of 2017 marks another valuable step forward — a recognition that the commercial vehicle segment, including heavy-duty vehicle OEMs, their tier 1 suppliers, telematics providers, and freight carriers can both benefit from and bring value to the Auto-ISAC.

"We look forward to welcoming our commercial vehicle counterparts to become members of Auto-ISAC," said Larry Hilke, Chair of Auto-ISAC's Affiliate Advisory Board and product cybersecurity leader for Cummins, Inc. "The growing number of synergies between the OEMs, the supply chain, and the commercial carriers will provide greater efficiencies in advancing cybersecurity protections."

This marks a key milestone for the automotive industry, where each of these member groups use the same connectivity technologies to build their resiliency. "Adding the commercial vehicle segment will strengthen Auto-ISAC's mission to support the industry's proactive efforts to incorporate strong security measures into every phase of vehicle development and operations," said Tom Stricker of Toyota, who serves as the organization's Chair.

Auto-ISAC collaborates with stakeholders across the commercial vehicle space, including industry groups, such as the National Motor Freight Traffic Association, Inc., to ensure a smooth integration and successful transition to a more connected mode of transportation. Extending membership across different segments of the connected vehicle ecosystem will keenly broaden the focus and increase insight in early detection and mitigation.

"Commercial vehicles play a critical role in our nation's delivery of services and goods," says Paul Levine, executive director of the National Motor Freight Traffic Association. "Proactively working together across the industry is key to making progress in protecting connected vehicles, large and small, against cybersecurity threats."

Auto-ISAC was formed in August 2015 by automakers to establish a secure platform for sharing, tracking and analyzing intelligence about cyber threats and potential vulnerabilities around the connected vehicle. Auto-ISAC operates as a central hub that allows members to anonymously submit and receive information to help them more effectively counter cyber threats in real time. Currently, Auto-ISAC members account for more than 99 percent of light-duty vehicles on the road in North America. It also has global representation from companies in Europe and Asia.

Auto-ISAC published the Automotive Cybersecurity Best Practices Executive Summary which outlines Auto-ISAC's development of informational guides that cover organizational and technical aspects of vehicle cybersecurity, including governance, risk management, security by design, threat detection, incident response, training, and collaboration with appropriate third parties.

Related Links

<https://www.automotiveisac.com/>