Auto-ISAC Releases Updated “Best Practice Guides” for Automotive Community

Navigating Today’s Complex Cybersecurity Landscape

WASHINGTON, DC, UNITED STATES, April 2, 2025 /EINPresswire.com/ -- The Automotive Information Sharing and Analysis Center (Auto-ISAC) today announced the release of its updated Best Practice Guides (BPGs), offering expert insights and effective approaches to enhance the cybersecurity of automotive vehicles, products, and technology.

The BPGs were built upon a solid foundation from the first set of guides, and extensive expertise of Auto-ISAC’s global membership, which includes 80 automotive companies. Developed collaboratively, these guides provide critical cybersecurity functions to assist automotive industry stakeholders in identifying, prioritizing, addressing, and monitoring cybersecurity risks.

"The Auto-ISAC benefits from a wealth of knowledge and expertise contributed by our diverse global membership — including manufacturers, suppliers, service providers, and fleet operators — who collaboratively developed these Best Practice Guides. As one of the most frequently accessed resources on our website, these guides offer invaluable insights to help strengthen automotive cybersecurity," said Kevin Tierney, Chairman of Auto-ISAC and Vice President at General Motors.

Evolving to Meet Industry Needs

When the Auto-ISAC formed, one of its first work products was a set of BPGs issued in 2016 through 2017. These seven guides were built before some of the cybersecurity standards and regulatory initiatives. With the cybersecurity environment continuing to evolve, novel approaches are being developed to meet emerging needs and challenges posed by the dynamic threats. As a result, in 2023 Auto-ISAC members recognized the need for further enhancements and initiated a comprehensive review. The result is a more streamlined and relevant set of guides that incorporates methodologies, along with lessons learned from recent industry developments, and aligns to published standards and regulations.
The Best Practice Guides are designed to support stakeholders across the automotive ecosystem in addressing cybersecurity risk and resiliency for the entire product, information technology (IT), and operational technology (OT) lifecycles. The guides provide actionable practices for every phase from design and development to deployment and decommissioning of systems, hardware, and software. Organizations are encouraged to adopt the practices that align most

effectively with their unique systems, processes, and risks, implementing them to fit their needs and priorities.

Key Focus Areas

The 2025 Best Practice Guides focus on five essential areas of cybersecurity:

1. Management and operations: Effective vulnerability management strengthens the automotive ecosystem by addressing security weaknesses across vehicles, infrastructure, and supply chains.

2. Awareness and training: Continuous cybersecurity awareness and comprehensive training empower employees to identify risks, adopt effective best practices, and foster a culture of security.

3. Governance, risk, and compliance: Strong oversight, effective risk management, and regulatory compliance are essential for navigating cybersecurity challenges.

4. Third-party risk management: Vehicle manufacturers depend on a vast network of suppliers, forming the backbone of the modern automotive supply chain. This reliance makes managing third-party cybersecurity risks a critical priority.

5. Secure development lifecycle: Integrating cybersecurity into every stage of the software development process enhances product security from inception to release.

Collaborative Development

Over a span of two years, Auto-ISAC members applied their specialized knowledge to update the guides. The Auto-ISAC's Education and Training Standing Committee initiated workshops to identify needed updates. Then a dedicated Best Practices Working Group formed specifically to provide the requisite expertise and experience to produce the updated BPGs.

The Working Group focused on reorganizing and adapting material from the earlier guides to enhance the overall effectiveness and efficiency of these resources. The 2016-17 BPGs listed seven best practices, and after review, the Working Group consolidated from seven to five to better address the evolving automotive cybersecurity landscape.

Upcoming Engagements

Members of the Best Practices Working Group will discuss the updated guides during the Auto-ISAC Monthly Community Call on May 7, 2025, at 11 AM ET. Contact us to participate in our monthly community calls.

In addition to the BPGs, further resources are now available at www.AutomotiveISAC.com. In

February 2025, Auto-ISAC released its trailblazing Auto-ISAC Software Bill of Materials (SBOM) Informational Report with effective practices to enhance the software security of automotive vehicles, products, and technology. The Third Annual Auto-ISAC European Cybersecurity Summit, taking place May 6-8, 2025, in Gothenburg, Sweden, is open for registration and sponsorships.

For more information, please visit our website or contact us directly.

About Auto-ISAC

Founded by automakers in 2015, the Auto-ISAC serves as a global information-sharing community dedicated to enhancing automotive cybersecurity. Acting as a central hub, it facilitates the sharing, tracking, and analysis of intelligence on emerging cyber threats against the automotive ecosystem. Auto-ISAC members represent over 99% of light-duty vehicles on North American roads, alongside heavy-duty vehicles, commercial fleets, carriers, and suppliers. European operations and staff supports our European members in their region and the Auto-ISAC collaborates closely with the Japan Auto-ISAC. For more information, please visit our website at www.automotiveisac.com and follow us on Linkedin.

Michael Shokouhi
Auto-ISAC
michaelshokouhi@automotiveisac.com
Visit us on social media:
LinkedIn

This press release can be viewed online at: https://www.einpresswire.com/article/798119957

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.
© 1995-2025 Newsmatics Inc. All Right Reserved.