



WELCOME TO AUTO-ISAC!

MONTHLY VIRTUAL COMMUNITY CALL





April 6, 2022

This Session will be recorded.

TLP:WHITE



DHS TRAFFIC LIGHT PROTOCOL (TLP) CHART

COLOR	WHEN SHOULD IT BE USED?	HOW MAY IT BE SHARED?
<p>TLP:RED</p>  <p>Not for disclosure, restricted to participants only.</p>	<p>Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.</p>	<p>Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.</p>
<p>TLP:AMBER</p>  <p>Limited disclosure, restricted to participants organizations.</p>	<p>Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.</p>	<p>Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. Sources are at liberty to specify additional intended limits of the sharing; these must be adhered to.</p>
<p>TLP:GREEN</p>  <p>Limited disclosure, restricted to the community.</p>	<p>Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.</p>	<p>Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.</p>
<p>TLP:WHITE</p>  <p>Disclosure is not limited.</p>	<p>Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.</p>	<p>Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.</p>

From: <https://www.us-cert.gov/tlp>

AGENDA

Time (ET)	Topic
11:00	Welcome <ul style="list-style-type: none">➤ Why We're Here➤ Expectations for This Community
11:05	Auto-ISAC Update <ul style="list-style-type: none">➤ Auto-ISAC Activities➤ Heard Around the Community➤ What's Trending
11:15	<i>DHS CISA Community Update</i>
11:20	Featured Speaker: <ul style="list-style-type: none">▪ <i>Tara Hairston, Senior Director, Alliance for Automotive Innovation</i>
11:45	Around the Room <ul style="list-style-type: none">➤ Sharing Around the Virtual Room
11:55	Closing Remarks

WELCOME - AUTO-ISAC COMMUNITY CALL!

Purpose: These monthly Auto-ISAC Community Meetings are an opportunity for you, our Members & connected vehicle ecosystem Partners, to:

- ✓ *Stay informed of Auto-ISAC activities*
- ✓ *Share information on key vehicle cybersecurity topics*
- ✓ *Learn about exciting initiatives within the automotive community from our featured speakers*

Participants: Auto-ISAC Members, Potential Members, Strategic Partners, Academia, Industry Stakeholders and Government – *the whole of the automotive industry*

Classification Level: **TLP:GREEN** - May be shared within the Auto-ISAC Community and “off the record”

How to Connect: For further info, questions or to add other POCs to the invite, please contact us!

(sharmilakhadka@automotiveisac.com)



ENGAGING IN THE AUTO-ISAC COMMUNITY

❖ Join

- ❖ If your organization is eligible, apply for Auto-ISAC Membership
- ❖ If you aren't eligible for Membership, connect with us as a Partner
- ❖ Get engaged – *“Cybersecurity is everyone's responsibility!”*



❖ Participate

- ❖ Participate in monthly virtual conference calls (1st Wednesday of month)
- ❖ If you have a topic of interest, let us know!
- ❖ Engage & ask questions!

22
OEM Members

21
Navigator Partners

❖ Share – *“If you see something, say something!”*

- ❖ Submit threat intelligence or other relevant information
- ❖ Send us information on potential vulnerabilities
- ❖ Contribute incident reports and lessons learned
- ❖ Provide best practices around mitigation techniques

43 *Supplier & Commercial Vehicle Members*

13
Innovator Partners

*Membership represents **99%** of cars and trucks on the road in North America*

*Coordination with **26** critical infrastructure ISACs through the National Council of ISACs (NCI)*



2022 - 2023 BOARD OF DIRECTORS

EXECUTIVE COMMITTEE (EXCOM)



Josh Davis
*Chair of the
Board of the Directors*
Toyota



Kevin Tierney
*Vice Chair of the
Board of the Directors*
GM



Jenny Gilger
*Secretary of the
Board of the Directors*
Honda



Tim Geiger
*Treasurer of the
Board of the Directors*
Ford



Todd Lawless
*Chair of the
Advisory Board*
Continental

2022-2023 ADVISORY BOARD (AB) LEADERSHIP



Todd Lawless
*Chair of the
Advisory Board*
Continental



Bob Kaster
*Vice Chair of the
Advisory Board*
Bosch



Allen Houck
Chair of the SAG
NXP



Larry Hilken
Chair of the CAG
Cummins

MEMBER ROSTER

AS OF APRIL 1, 2022

66 Members, 4 in Progress

Highlight = Change

Aisin	Hyundai	Nuro
Allison Transmission	Infineon	NXP
Aptiv	Intel	Oshkosh Corp
Argo AI, LLC	John Deere Electronic	PACCAR
AT&T	Kia	Panasonic (Ficosa-Affiliate)
AVL List GmbH	Knorr Bremse	Polaris
Blackberry Limited	Lear	Qualcomm
BMW Group	LGE	Renesas Electronics
BorgWarner	Lucid Group	Stellantis
Bosch (Ecrypt-Affiliate)	Luminar	Subaru
Continental (Argus-Affiliate)	Magna	Sumitomo Electric
Cummins	MARELLI	Tokai Rika
Denso	Mazda	Toyota (Woven Planet – Affiliate)
Faurecia	Mercedes-Benz	TuSimple
Ford	Meritor	Valeo
Garrett	Mitsubishi Motors	Veoneer
General Motors (Cruise-Affiliate)	Mitsubishi Electric	Volkswagen
Geotab	Mobis	Volvo Cars
Google	Motional	Volvo Group
Harman	Navistar	Waymo
Hitachi	Nexteer Automotive Corp	Yamaha Motors
Honda	Nissan	ZF

UPCOMING EVENTS

➤ Community Call:

- Wednesday, May 4 - **Speaker:** Kenneth J. Peterson, CTPRP, Founder and CEO, Churchill & Harriman, Inc.
- **Title:** “Protecting and Enabling Global Revenue Streams ” **Time:** 11 – 12:00 p.m. **TLP:WHITE**

➤ Members Teaching Members:

- Wednesday, April 20 – **Speaker:** Brian Witten, Aptiv **Title:** Compare & Contrast Automotive Product Security with Aerospace, Medical, Industrial Controls & More **Time:** 10 – 11:30 a.m. **TLP:AMBER**

➤ Announcements:

- *****New Auto-ISAC Website launched.** Contact [Michael Shokouhi](#) if you have any feedback.
- **Call for Community Call Speakers:** Might you want to speak on the topics related to Automotive and Cybersecurity? Please send your ideas to [Sharmila Khadka](#).
- Board approved the **SAG's SBOM's** material as an **Information Report for release to Members only** at this time. **SAG's SBoM WG targeting a broader release in 3Q2022.**
- **2021 Auto-ISAC Annual Report:** Board Approved. Currently preparing **TLP: GREEN** for dissemination in May.
- **ACT Program Advanced Courses** begin on April 11th. Beta signup is open for **Members only now**. Contact [Tamara Shoemaker](#).



AUTO-ISAC INTELLIGENCE

TLP:WHITE



AUTO-ISAC INTELLIGENCE

- Know what we track daily by subscribing to the DRIVEN
 - **Send feedback**, contributions or questions to analyst@automotiveisac.com
- Expect the Auto-ISAC 2021 Annual Report and Threat Assessment soon.
- Intelligence Notes
 - Russia's war on Ukraine continues. Maintain heightened vigilance of your business networks, industrial systems, and products for the foreseeable future, **including after the war ends**.
 - As long as multinational economic and social marginalization of Russia persists, the heightened threat from the Russian government and pro-Russia criminal sympathizers will continue ([CISA Shields Up](#)).
 - Even before Russia attacked Ukraine, we were advising the automotive community to maintain heightened vigilance for signs of malicious activity or compromise in the existing threat environment. **The Russia threat merely adds to an already heightened threat environment** ([CISA-Known Exploited Vulnerabilities Catalog](#), [CISA-Technical Approaches to Uncovering and Remediating Malicious Activity](#)).
 - Almost every day we are seeing reports of various types of automotive companies being listed as ransomware victims on the dark web (along with organizations in other economic sectors). **Any** automotive company can be a victim **any day**. Prepare to respond and recover.

CISA RESOURCE HIGHLIGHTS



TLP: WHITE – CISA Industrial Control Systems Working Group (ICSJWG) Spring Virtual Event

- **ICSJWG Spring 2022 – Virtual Event – Tuesday and Wednesday April 26-27, 2022**
- **Save-the-date and registration links at:**
 - [https://www\[.\]cisa\[.\]gov/uscert/ics/icsjwg-meetings-and-webinars](https://www[.]cisa[.]gov/uscert/ics/icsjwg-meetings-and-webinars)
 - [https://www\[.\]cisa\[.\]gov/uscert/ics/Industrial-Control-Systems-Joint-Working-Group-ICSJWG](https://www[.]cisa[.]gov/uscert/ics/Industrial-Control-Systems-Joint-Working-Group-ICSJWG)
- **Contact ICSJWG at ICSJWG.Communications@cisa.dhs.gov**



TLP: WHITE – CISA Shields Up Website

- Provides resources and recommendations to prepare for, respond to, and mitigate the impact of cyber attacks
- Designed to support every organization – large and small – in their preparation to respond to disruptive cyber activity
- Technical Guidance page also available that provides information for review and consideration in responding to cyber incidents
- Resources available at:
 - [https://www\[.\]cisa\[.\]gov/shields-up](https://www[.]cisa[.]gov/shields-up)
 - [https://www\[.\]cisa\[.\]gov/uscert/shields-technical-guidance](https://www[.]cisa[.]gov/uscert/shields-technical-guidance)



TLP: WHITE – CISA Current Activities – Joint Products

- **Mitigating Attacks Against Uninterruptible Power Supply Devices – CISA, DOE**
 - [https://www\[.\]cisa\[.\]gov/uscert/ncas/current-activity/2022/03/29/mitigating-attacks-against-uninterruptible-power-supply-devices](https://www[.]cisa[.]gov/uscert/ncas/current-activity/2022/03/29/mitigating-attacks-against-uninterruptible-power-supply-devices)
 - [https://www\[.\]cisa\[.\]gov/sites/default/files/publications/CISA-DOE_Insights-Mitigating_Vulnerabilities_Affecting_Uninterruptible_Power_Supply_Devices_Mar_29.pdf](https://www[.]cisa[.]gov/sites/default/files/publications/CISA-DOE_Insights-Mitigating_Vulnerabilities_Affecting_Uninterruptible_Power_Supply_Devices_Mar_29.pdf)
- **State-Sponsored Russian Cyber Actors Targeted Energy Sector from 2011 to 2018 – CISA, FBI, DOE**
 - [https://www\[.\]cisa\[.\]gov/uscert/ncas/current-activity/2022/03/24/state-sponsored-russian-cyber-actors-targeted-energy-sector-2011](https://www[.]cisa[.]gov/uscert/ncas/current-activity/2022/03/24/state-sponsored-russian-cyber-actors-targeted-energy-sector-2011)
 - [https://www\[.\]cisa\[.\]gov/uscert/ncas/alerts/aa22-083a](https://www[.]cisa[.]gov/uscert/ncas/alerts/aa22-083a)



TLP: WHITE – CISA Current Activities – Joint Products - continued

- **Strengthening Cybersecurity of SATCOM Network Providers and Customers – CISA, FBI**
- [https://www\[.\]cisa\[.\]gov/uscert/ncas/current-activity/2022/03/17/strengthening-cybersecurity-satcom-network-providers-and-customers](https://www[.]cisa[.]gov/uscert/ncas/current-activity/2022/03/17/strengthening-cybersecurity-satcom-network-providers-and-customers)
- [https://www\[.\]cisa\[.\]gov/uscert/ncas/alerts/aa22-076a](https://www[.]cisa[.]gov/uscert/ncas/alerts/aa22-076a)
- **Updated: Kubernetes Hardening Guide – NSA, CISA**
 - [https://www\[.\]cisa\[.\]gov/uscert/ncas/current-activity/2022/03/15/updated-kubernetes-hardening-guide](https://www[.]cisa[.]gov/uscert/ncas/current-activity/2022/03/15/updated-kubernetes-hardening-guide)
 - [https://media\[.\]defense\[.\]gov/2021/Aug/03/2002820425/-1/-1/0/CTR_Kubernetes_Hardening_Guidance_1.1_20220315.PDF](https://media[.]defense[.]gov/2021/Aug/03/2002820425/-1/-1/0/CTR_Kubernetes_Hardening_Guidance_1.1_20220315.PDF)



TLP: WHITE – CISA Current Activities – Joint Products - continued

- **Russian State-Sponsored Cyber Actors Access Network Misconfigured with Default MFA Protocols – CISA, FBI**
- [https://www\[.\]cisa\[.\]gov/uscert/ncas/current-activity/2022/03/15/russian-state-sponsored-cyber-actors-access-network-misconfigured](https://www[.]cisa[.]gov/uscert/ncas/current-activity/2022/03/15/russian-state-sponsored-cyber-actors-access-network-misconfigured)
- [https://www\[.\]cisa\[.\]gov/uscert/ncas/alerts/aa22-074a](https://www[.]cisa[.]gov/uscert/ncas/alerts/aa22-074a)
- **Updated: Conti Ransomware – CISA, FBI, NSA, USSS**
 - [https://www\[.\]cisa\[.\]gov/uscert/ncas/current-activity/2022/03/09/updated-conti-ransomware](https://www[.]cisa[.]gov/uscert/ncas/current-activity/2022/03/09/updated-conti-ransomware)
 - [https://www\[.\]cisa\[.\]gov/uscert/ncas/alerts/aa21-265a](https://www[.]cisa[.]gov/uscert/ncas/alerts/aa21-265a)



TLP: WHITE – Two Hundred Twenty-Six (226) Known Exploited Vulnerabilities added in March 2022

- **The following CISA Current Activities highlight added KEVs:**
 - [https://www\[.\]cisa\[.\]gov/uscert/ncas/current-activity/2022/03/31/cisa-adds-seven-known-exploited-vulnerabilities-catalog](https://www[.]cisa[.]gov/uscert/ncas/current-activity/2022/03/31/cisa-adds-seven-known-exploited-vulnerabilities-catalog)
 - [https://www\[.\]cisa\[.\]gov/uscert/ncas/current-activity/2022/03/28/cisa-adds-32-known-exploited-vulnerabilities-catalog](https://www[.]cisa[.]gov/uscert/ncas/current-activity/2022/03/28/cisa-adds-32-known-exploited-vulnerabilities-catalog)
 - [https://www\[.\]cisa\[.\]gov/uscert/ncas/current-activity/2022/03/25/cisa-adds-66-known-exploited-vulnerabilities-catalog](https://www[.]cisa[.]gov/uscert/ncas/current-activity/2022/03/25/cisa-adds-66-known-exploited-vulnerabilities-catalog)
 - [https://www\[.\]cisa\[.\]gov/uscert/ncas/current-activity/2022/03/15/cisa-adds-15-known-exploited-vulnerability-catalog](https://www[.]cisa[.]gov/uscert/ncas/current-activity/2022/03/15/cisa-adds-15-known-exploited-vulnerability-catalog)
 - [https://www\[.\]cisa\[.\]gov/uscert/ncas/current-activity/2022/03/07/cisa-adds-11-known-exploited-vulnerabilities-catalog](https://www[.]cisa[.]gov/uscert/ncas/current-activity/2022/03/07/cisa-adds-11-known-exploited-vulnerabilities-catalog)
 - [https://www\[.\]cisa\[.\]gov/uscert/ncas/current-activity/2022/03/03/cisa-adds-95-known-exploited-vulnerabilities-catalog](https://www[.]cisa[.]gov/uscert/ncas/current-activity/2022/03/03/cisa-adds-95-known-exploited-vulnerabilities-catalog)
- **KEV Catalog:**
 - [https://www\[.\]cisa\[.\]gov/known-exploited-vulnerabilities-catalog](https://www[.]cisa[.]gov/known-exploited-vulnerabilities-catalog)



TLP: WHITE – Additional Resources From CISA

- CISA Homepage - [https://www\[.\]cisa\[.\]gov/](https://www[.]cisa[.]gov/)
- CISA NCAS – [https://us-cert\[.\]cisa\[.\]gov/](https://us-cert[.]cisa[.]gov/)
- CISA Shields Up - [https://www\[.\]cisa\[.\]gov/shields-up](https://www[.]cisa[.]gov/shields-up)
- Free Cybersecurity Services and Tools - [https://www\[.\]cisa\[.\]gov/free-cybersecurity-services-and-tools](https://www[.]cisa[.]gov/free-cybersecurity-services-and-tools)
- CISA News Room - [https://www\[.\]cisa\[.\]gov/cisa/newsroom](https://www[.]cisa[.]gov/cisa/newsroom)
- CISA Blog - [https://www\[.\]cisa\[.\]gov/blog-list](https://www[.]cisa[.]gov/blog-list)
- CISA Publications Library - [https://www\[.\]cisa\[.\]gov/publications-library](https://www[.]cisa[.]gov/publications-library)
- CISA Cyber Resource Hub - [https://www\[.\]cisa\[.\]gov/cyber-resource-hub](https://www[.]cisa[.]gov/cyber-resource-hub)
- CISA Cybersecurity Directives - [https://cyber\[.\]dhs\[.\]gov/directives/](https://cyber[.]dhs[.]gov/directives/)





For more information:
[cisa.gov](https://www.cisa.gov)

Questions?
Central@cisa.dhs.gov
1-888-282-0870



AUTO-ISAC COMMUNITY MEETING

Why Do We Feature Speakers?

- ❖ These calls are an opportunity for information exchange & learning
- ❖ Goal is to educate & provide awareness around cybersecurity for the *connected vehicle*

What Does it Mean to Be Featured?

- ❖ Perspectives across our ecosystem are shared from Members, government, academia, researchers, industry, associations and others.
- ❖ Goal is to showcase a rich & balanced variety of topics and viewpoints
- ❖ *Featured speakers are not endorsed by Auto-ISAC nor do the speakers speak on behalf of Auto-ISAC*

How Can I Be Featured?

- ❖ If you have a topic of interest you would like to share with the broader Auto-ISAC Community, then we encourage you to contact us!

30+
*Featured
Speakers to
date*

7 *Best
Practice
Guides
available on
website*

2000+
*Community
Participants*





FEATURED SPEAKER

TLP:WHITE



TARA HAIRSTON, ALLIANCE FOR AUTOMOTIVE INNOVATION

SENIOR DIRECTOR, TECHNOLOGY, INNOVATION, & MOBILITY POLICY

Tara Hairston supports policy development on technology, innovation, and mobility policy issues, including artificial intelligence, cybersecurity, intellectual property rights protection, emerging transportation technologies, and new mobility models.

Prior to joining Auto Innovators, Tara spent over five years as the Head of Government Relations, North America for Kaspersky and nearly a decade working on federal and state policy at Honda.

Tara holds a double B.A. in Political Science and International Relations from Saint Joseph's College, New York.



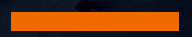
<https://www.autosinnovate.org/>

AfAI Mission

***Cleaner. Safer. Smarter.** Formed by the 2020 combination of the Alliance of Automobile Manufacturers (Auto Alliance) and the Association of Global Automakers (Global Automakers), Auto Innovators is dedicated to propelling the unprecedented innovation that will make our lives better. Driven by the collective energy of the world's multi-faceted auto industry, we are on the leading edge of transforming personal mobility, in a cleaner, safer, and smarter manner.*

Cybersecurity Policy Developments for the Auto Industry

April 6, 2022



ALLIANCE
FOR AUTOMOTIVE
INNOVATION

TODAY'S ROADMAP

AGENDA

- **Brief Introduction**
- **Cybersecurity Incident Reporting**
- **Cybersecurity Governance**
- **Supply Chain Risk Management**
- **Questions & Answers**

What is the Alliance for Automotive Innovation?

Auto Innovators is...

The singular, authoritative, and respected voice of the automotive industry. Focused on creating a safe and transformative path for sustainable industry growth, the Alliance for Automotive Innovation represents the manufacturers producing nearly 98 percent of cars and light trucks sold in the U.S. The organization is involved in regulatory and policy matters impacting the light-duty vehicle market across the country. Members include U.S. operations of international motor vehicle manufacturers, original equipment suppliers, technology, and other automotive-related companies and trade associations.

CYBERSECURITY INCIDENT REPORTING

New Law

FY22 Omnibus
Appropriations bill
signed March 15, 2022

Cyber Incident
Reporting for Critical
Infrastructure Act of
2022 now law

Pending CISA
Rulemaking Process

Proposed Regulation

SEC Proposed Rule on
March 9, 2022

Comments Due May 9,
2022

Final Outcome ???

Why this Matters...

- **Applicability and Scope**
- **Multiple reporting timelines**
- **Potentially inconsistent reporting content requirements**
- **Potential lack of harmonization between recipient agencies**

CYBERSECURITY GOVERNANCE

Recent Calls for Enhanced Cybersecurity Governance...



- SEC Proposed Rules
- CISA Letter to NACD
- NIST CSF 2.0

SUPPLY CHAIN RISK MANAGEMENT

Supply Chain, Supply Chain...

Secure Software Development Framework

SEC Proposed Rule

Software Bill of Materials

Cybersecurity Executive Order 14028

National Initiative for Improving Cybersecurity in Supply Chains

White House Announcement

NIST SP 800-161

QUESTIONS?



ALLIANCE
FOR AUTOMOTIVE
INNOVATION

Transforming Personal Mobility

OPEN DISCUSSION

*ANY QUESTIONS ABOUT THE AUTO-ISAC OR FUTURE
TOPICS FOR DISCUSSION?*

HOW TO GET INVOLVED: MEMBERSHIP

IF YOU ARE AN OEM, SUPPLIER OR COMMERCIAL VEHICLE, CARRIER OR FLEET, PLEASE JOIN THE AUTO-ISAC!

- *REAL-TIME INTELLIGENCE SHARING*
- *INTELLIGENCE SUMMARIES*
- *REGULAR INTELLIGENCE MEETINGS*
- *CRISIS NOTIFICATIONS*
- *MEMBER CONTACT DIRECTORY*
- *DEVELOPMENT OF BEST PRACTICE GUIDES*
- *EXCHANGES AND WORKSHOPS*
- *TABLETOP EXERCISES*
- *WEBINARS AND PRESENTATIONS*
- *ANNUAL AUTO-ISAC SUMMIT EVENT*

**To learn more about Auto-ISAC Membership, please contact andreaschunn@automotiveisac.com.
For Partnership, please contact sharmilakhadka@automotiveisac.com.**

AUTO-ISAC PARTNERSHIP PROGRAMS

Strategic Partnership

- **For-profit** companies such as “Solutions Providers” that sell connected vehicle cybersecurity products & services.
 - **Examples:** *Hacker ONE, Upstream, IOActive, Karamba, Grimm*
1. **Must be approved** by Executive Director and the Membership & Benefit Standing Committee (MBSC).
 2. Formal agreements: **NDA, SPA, SoW, CoC** required.
 3. **In-kind contributions** allowed. Currently no fee.
 4. **Does not** overtly sell or promote product or service.
 5. Commits to **support the Auto-ISAC’s mission**.
 6. Engages with the automotive ecosystem, **supporting & educating Auto-ISAC Members and its Community**.
 7. **Develops value added Partnership Projects** to engage with the Auto-ISAC, its Member, and Community.
 8. **Summit Sponsorship** allowed for promotion. Summit Booth **priority**.
 9. Engagement **must provide Member awareness, education, training, and information sharing**
 10. **Builds relationships, shares, and participates** in information sharing Auto-ISAC activities.
 11. Supports our mission through **educational webinars and sharing of information**.

Community Partnership

- **Community Partners** are companies, individuals, or organizations with a complementary mission to the Auto-ISAC, with the interest in engaging with the automotive ecosystem, supporting, and educating Members and the community.
 - Includes **Industry Associations, Government Partners, Academia, Research Institution, Standards Organizations, Non-Profit, Technical Experts, Auto-ISAC Sponsors**.
 - **Examples:** *Autos Innovate, ATA, ACEA, JAMA, MEMA, CLEPA, CISA, DHS, FBI, NHTSA, NCI, UDM etc.*
1. **No formal agreement** required.
 2. **No approval** required.
 3. Added to **Auto-ISAC Community Distro** List to stay engaged in Community events and activities.
 4. Participate in **Auto-ISAC Monthly Community Calls**.
 5. Learn **what is trending** in the ISACs and hear from key leaders during the **special topic of interest** presentation.
 6. Added to **Auto-ISAC DRIVEN** list to receive our **daily cyber automotive newsletter**.
 7. Part of the Network with **Automotive Community and the extended automotive ecosystem**.
 8. Invitation to **attend and support** our yearly Summit.

CURRENT PARTNERSHIPS

MANY ORGANIZATIONS ENGAGING

Thanks for your Support to our Many Partners

COMMUNITY PARTNERS

INNOVATOR

**Strategic Partnership
(13)**

Cybellum
Deloitte
FEV
GRIMM
HackerOne
Karamba Security
Kela
Pen Testing Partners
Red Balloon Security
Regulus Cyber
Saferide
Security Scorecard
Upstream

NAVIGATOR

Support Partnership

AAA
ACEA
ACM
American Trucking
Associations (ATA)
ASC
ATIS
Auto Alliance
EMA
Global Automakers
IARA
IIC
JAMA
MEMA
NADA
NAFA
NMFTA
RVIA
SAE
TIA
Transport Canada

COLLABORATOR

**Coordination
Partnership**

AUTOSAR
Billington Cybersecurity
Cal-CSIC
Computest
Cyber Truck Challenge
DHS CSVI
DHS HQ
DOT-PIF
FASTR
FBI
GAO
ISAO
Macomb Business/MADCAT
Merit (training, np)
MITRE
National White Collar Crime Center
NCFTA
NDIA
NHTSA
NIST
Northern California Regional Intelligence
Center (NCRIC)
NTIA - DoCommerce
OASIS
ODNI
Ohio Turnpike & Infrastructure Commission
SANS
The University of Warwick
TSA
University of Tulsa
USSC
VOLPE
W3C/MIT
Walsch College

BENEFACTOR

**Sponsorship
Partnership**

2021 Summit Sponsors-

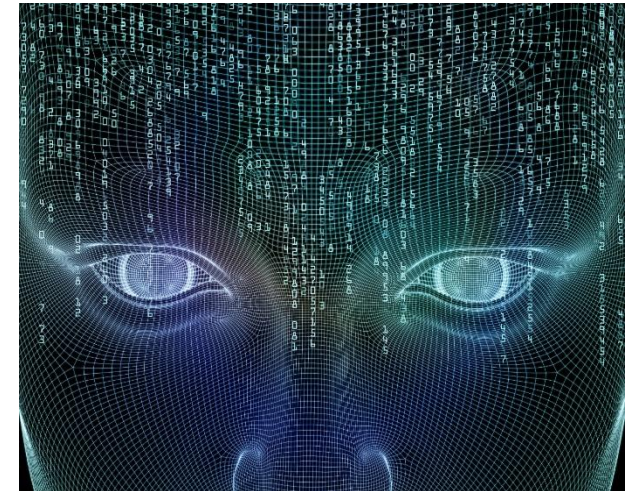
Celerium
Cyware
Denso
NDIAS
IOActive
Claroty
Deloitte
Finite State
Tanium
Recorded Future
PaloAlto Networks
Upstream
Securonix
Zimperium
Micron
Block Harbor
SecurityScorecard
Booz Allen
CybelAngel
ATT
Ford
Cybellum

2020 Summit Sponsors-

Claroty
Upstream
Escrypt
Blackberry
Cybellum
Blockharbor
C2A
Synopsis
Intsignts
ValiMail

AUTO-ISAC BENEFITS

- Focused Intelligence Information/Briefings
- Cybersecurity intelligence sharing
- Vulnerability resolution
- Member to Member Sharing
- Distribute Information Gathering Costs across the Sector
- Non-attribution and Anonymity of Submissions
- Information source for the entire organization
- Risk mitigation for automotive industry
- Comparative advantage in risk mitigation
- Security and Resiliency



Building Resiliency Across the Auto Industry

THANK YOU!



OUR CONTACT INFO

Faye Francy
Executive Director



20 F Street NW, Suite 700
Washington, DC 20001
703-861-5417
fayefrancy@automotiveisac.com

Sharmila Khadka
Information Technology Executive
Coordinator



20 F Street NW, Suite 700
Washington, DC 20001
443-962-5663
sharmilakhadka@automotiveisac.com



www.automotiveisac.com
[@auto-ISAC](https://twitter.com/auto-ISAC)