Welcome to Auto-ISAC!

Monthly Virtual Community Call

November 2nd, 2022
This Session will be recorded.

TLP: WHITE
## DHS Traffic Light Protocol (TLP) Chart

<table>
<thead>
<tr>
<th>COLOR</th>
<th>WHEN SHOULD IT BE USED?</th>
<th>HOW MAY IT BE SHARED?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>TLP:RED</strong></td>
<td>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.</td>
<td>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.</td>
</tr>
<tr>
<td>Not for disclosure, restricted to participants only.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>TLP:AMBER</strong></td>
<td>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.</td>
<td>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.</td>
</tr>
<tr>
<td>Limited disclosure, restricted to participants organizations.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>TLP:GREEN</strong></td>
<td>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.</td>
<td>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.</td>
</tr>
<tr>
<td>Limited disclosure, restricted to the community.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>TLP:WHITE</strong></td>
<td>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.</td>
<td>Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.</td>
</tr>
<tr>
<td>Disclosure is not limited.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*From: https://www.us-cert.gov/tlp*
# Agenda

<table>
<thead>
<tr>
<th>Time (ET)</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>11:00</td>
<td>Welcome</td>
</tr>
<tr>
<td></td>
<td>- Why We’re Here</td>
</tr>
<tr>
<td></td>
<td>- Expectations for This Community</td>
</tr>
<tr>
<td>11:05</td>
<td>Auto-ISAC Update</td>
</tr>
<tr>
<td></td>
<td>- Auto-ISAC Activities</td>
</tr>
<tr>
<td></td>
<td>- Heard Around the Community</td>
</tr>
<tr>
<td></td>
<td>- Intelligence Highlights</td>
</tr>
<tr>
<td>11:15</td>
<td>DHS CISA Community Update</td>
</tr>
<tr>
<td>11:20</td>
<td>Featured Speaker:</td>
</tr>
<tr>
<td></td>
<td>- Brandon Barry, CEO, Block Harbor Cybersecurity</td>
</tr>
<tr>
<td></td>
<td>- Title: “A Global Grassroots Community of 10,000+ Automotive Security Folks: The ASRG”</td>
</tr>
<tr>
<td>11:45</td>
<td>Around the Room</td>
</tr>
<tr>
<td></td>
<td>- Sharing Around the Virtual Room</td>
</tr>
<tr>
<td>11:55</td>
<td>Closing Remarks</td>
</tr>
</tbody>
</table>
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!

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

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)

26 OEM Members
21 Navigator Partners
49 Supplier & Commercial Vehicle Members
18 Innovator Partners

Innovator Partners
Navigator Partners
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

Bob Kaster
Vice Chair of the Advisory Board
Bosch

TBA
Chair of the SAG
TBA

Larry Hilkene
Chair of the CAG
Cummins

2022-2023 Advisory Board (AB) Leadership

Todd Lawless
Chair of the Advisory Board
Continental

Bob Kaster
Vice Chair of the Advisory Board
Bosch

TBA
Chair of the SAG
TBA

Larry Hilkene
Chair of the CAG
Cummins

Thanks to Allen Houck, NXP for his service!
# Member Roster

**As of November 2022**

<table>
<thead>
<tr>
<th>Highlight = Change</th>
<th>75 Members, 3 in Progress</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Aisin</th>
<th>Ferrari</th>
<th>Magna</th>
<th>Qualcomm</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allison Transmission</td>
<td>Flex</td>
<td>MARELLI</td>
<td>Renesas Electronics</td>
</tr>
<tr>
<td>American Axle &amp; Manufacturing</td>
<td>Ford</td>
<td>Mazda</td>
<td>Stellantis</td>
</tr>
<tr>
<td>Aptiv</td>
<td>Garrett</td>
<td>Mercedes-Benz</td>
<td>Subaru</td>
</tr>
<tr>
<td>Argo AI, LLC</td>
<td>General Motors (Cruise-Affiliate)</td>
<td>Meritor</td>
<td>Sumitomo Electric</td>
</tr>
<tr>
<td>AT&amp;T</td>
<td>Geotab</td>
<td>Mitsubishi Electric</td>
<td>Tokai Rika</td>
</tr>
<tr>
<td>AVL List GmbH</td>
<td>Harman</td>
<td>Mitsubishi Motors (Woven Planet-Affiliate)</td>
<td>Toyota</td>
</tr>
<tr>
<td>Blackberry Limited</td>
<td>Hitachi</td>
<td>Mobis</td>
<td>TuSimple</td>
</tr>
<tr>
<td>BMW Group</td>
<td>Honda</td>
<td>Motional</td>
<td>thyssenkrupp</td>
</tr>
<tr>
<td>BorgWarner</td>
<td>Hyundai</td>
<td>Navistar</td>
<td>Valeo</td>
</tr>
<tr>
<td>Bosch (Escrypt-Affiliate)</td>
<td>Infineon</td>
<td>Nexteer Automotive Corp</td>
<td>Veoneer</td>
</tr>
<tr>
<td>Canoo</td>
<td>Intel</td>
<td>Nissan</td>
<td>Vitesco</td>
</tr>
<tr>
<td>ChargePoint</td>
<td>John Deere Electronic</td>
<td>Nuro</td>
<td>Volkswagen</td>
</tr>
<tr>
<td>Continental (Argus-Affiliate)</td>
<td>Kia</td>
<td>Nuspire</td>
<td>Volvo Cars</td>
</tr>
<tr>
<td>Cummins</td>
<td>Knorr Bremse</td>
<td>NXP</td>
<td>Volvo Group</td>
</tr>
<tr>
<td>Cymotive</td>
<td>Lear</td>
<td>Oshkosh Corp</td>
<td>Waymo</td>
</tr>
<tr>
<td>Denso</td>
<td>LG Electronics</td>
<td>PACCAR</td>
<td>Yamaha Motors</td>
</tr>
<tr>
<td>e:fs</td>
<td>Lucid Motors</td>
<td>Panasonic (Ficosa-Affiliate)</td>
<td>ZF</td>
</tr>
<tr>
<td>Faurecia</td>
<td>Luminar</td>
<td>Polaris</td>
<td></td>
</tr>
</tbody>
</table>

Pending: KTM, Micron, Rivian
Upcoming Events

Upcoming Meetings:
- **Community Call**: Wednesday, December 7th **Time**: 11 – 12:00 p.m. **TLP:WHITE**
  - **Title**: “CISCP to JCDC Transition”
  - **Speaker**:
    - James Murphy - Section Chief, Industry Partnerships | Joint Cyber Defense Collaborative (JCDC)
    - Dan Strachan - Senior Engagement Lead, Industry Partnerships | Joint Cyber Defense Collaborative (JCDC)
    - Pranav Julakanti - Consultant, Industry Partnerships | Joint Cyber Defense Collaborative (JCDC)

- **Members Teaching Members**:
  - **Wednesday, November 16th** – **Speaker**: Michael Schneider, ETAS GmbH, Senior Security Consultant
  - **Title**: “Securing Modern Vehicles with AUTOSAR” **Time**: 10 – 11:30 a.m. **TLP:AMBER** (Members Only)

Announcements:
- **ACT Program Advanced Courses** – Beta Advanced registration is open. Concepts and Compliance (Nov 1-4) is still open for registration. Contact Tamara Shoemaker. (Members Only)
- **Best Practice Guide Updates** – ETSC is kicking off a “Light Touch” Best Practice Guide update to bring the existing guides up to current references and standards.
Auto-ISAC Intelligence

- Know what we track daily: subscribe to the DRIVEN; know our strategic view of the cyber threat environment: read the TLP:GREEN Threat Assessment in our 2021 Annual Report
  - Send feedback, contributions, or questions to analyst@automotiveisac.com

- Intelligence Notes
  - Geopolitical tensions in key regions show no signs of abating:
    - Russia-Ukraine: In Crisis (The Hill, BBC)
    - China-Taiwan: High (Taiwan News, Eurasian Times)
    - North Korea-South Korea: High (Reuters, Aljazeera)
    - Iran: High (CNN, Reuters)
  - Russia, China, North Korea, and Iran have significant cyberattack capabilities which could manifest without warning and impact business and industrial operations (Russia, China, North Korea, Iran).
  - CISA-Technical Approaches to Uncovering and Remediating Malicious Activity*).
  - Ransomware Groups Targeting Automotive: RansomEXX, Vice Society, Black Basta.
  - Multiple incidents of threat actors selling access to automotive organizations’ networks and selling or leaking sensitive information.*
  - Notable Incidents, TTPs, and Tools: BlueBleed (Microsoft, Socradar); Unidentified Fraudulent Diagnostic Tool Used for Vehicle Theft (BleepingComputer); Targeting Shadow APIs (Cequence); Qbot Malware Deployment (Trend Micro); Azov Data Wiper (BleepingComputer); Mark-of-the-Web Bypass (BleepingComputer).
Sunsetting
CISCP
CISA, the Federal Bureau of Investigation (FBI), and the Multi-State Information Sharing and Analysis Center (MS-ISAC) have released a publication: Understanding and Responding to Distributed Denial-of-Service Attacks to provide organizations with proactive steps to reduce the likelihood and impact of distributed denial-of-service (DDoS) attacks. The guidance is for both network defenders and leaders to help them understand and respond to DDoS attacks, which can cost an organization time, money, and reputational damage.

A PDF of the guidance can be found here: https://www.cisa.gov/sites/default/files/publications/understanding-and-responding-to-ddos-attacks_508c.pdf

The announcement can be found here: Joint CISA FBI MS-ISAC Guide on Responding to DDoS Attacks and DDoS Guidance for Federal Agencies | CISA
CISA has released four (4) Industrial Control Systems (ICS) advisories on October 27, 2022. These advisories provide timely information about current security issues, vulnerabilities, and exploits surrounding ICS. CISA encourages users and administrators to review the newly released ICS advisory for technical details and mitigations:

- ICSA-22-300-01 Rockwell Automation FactoryTalk Alarm and Events Server | Rockwell Automation FactoryTalk Alarm and Events Server | CISA
- ICSA-22-300-02 SAUTER Controls moduWeb | CISA
- ICSA-22-300-03 Rockwell Automation Stratix Devices Containing Cisco IOS | CISA
- ICSA-22-300-04 VTScada | CISA
CISA strongly urges all organizations to reduce their exposure to cyberattacks by prioritizing timely remediation of Catalog vulnerabilities as part of their vulnerability management practice.

CISA has added 11 new vulnerabilities to its Known Exploited Vulnerabilities Catalog in the month of October. These types of vulnerabilities are a frequent attack vector for malicious cyber actors and pose significant risk to the federal enterprise.
Additional Resources from CISA

- CISA Homepage - https://www.cisa.gov/
- CISA NCAS – https://us-cert.cisa.gov/
- CISA Shields Up - https://www.cisa.gov/shields-up
- CISA News Room - https://www.cisa.gov/cisa/newsroom
- CISA Blog - https://www.cisa.gov/blog-list
- CISA Cybersecurity Directives - https://cyber.dhs.gov/directives/
For more information:
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

TLP:WHITE 8 November 2022
Featured Speaker
Meet the Speaker

Brandon Barry
Block Harbor Cybersecurity

Brandon Barry studied Computer Engineering with a research focus on vehicle cybersecurity at Brown University. He founded Block Harbor Cybersecurity in 2014 to support automakers and tier ones with solutions in vehicle cybersecurity where his role is CEO. His team placed first place at the DEF CON Car Hacking Village Capture the Flag in 2019 and second place in 2022. He has been invited to several private bug bounty events with automakers.

Brandon leads the Americas chapters of the ASRG with a focus on the Detroit chapter. Outside of the day job at Block Harbor and the ASRG, he’s passionate about cars with a focus on drift racing.
Automotive Security.
Community Driven.

A Global Grassroots Community of 10,000+ Automotive Security Folks: the ASRG
Agenda

01 My story
02 About the ASRG
03 What the ASRG’s up to
04 Get involved
05 ASRG-Detroit: Toy Drive & Shop Talk
   3PM-8PM on December 8, 2022 #FILLTHEFRUNK
ASRG Toy Drive & Shop Talk

December 8th, 2022
@Block Harbor: 1111 Bellevue Street, Detroit, MI 48207
3-8pm

Topic: I’m a Vehicle Cybersecurity Expert,
Change My Mind

#FILLTHEFRUNK

Food & Drink provided w/ a special guest visit
Admission: Free, but bring a toy or donate if you can

bit.ly/3Ue8lzM
Brandon Barry
About Me

Founder
Block Harbor Cybersecurity

Americas Lead
Automotive Security Research Group (NPO)

Self-Proclaimed Professional Drift Racer
My Story

How I got into Vehicle Cybersecurity

- 2014: Internship in cybersecurity, FCA
- Late 2014: Founded Block Harbor as an Undergrad at Brown University
  - Computer Engineering, research focus on Vehicle Cybersecurity
  - Early projects in:
    - VSOC
    - Vehicle System Risk Assessment
    - Vehicle System Penetration Testing
    - Vehicle Cybersecurity Automated Testing
- 2015: Vehicle Cybersecurity, front and center in the media
- Tinkered with my own car
- 2016: J3061, Car Hacker’s Handbook
- 2018: Graduated, came back to Detroit to really tackle problems in Vehicle Cybersecurity full time
- 2019: DEF CON Car Hacking Village CTF 1st Place, CANucks
- 2020: The standard and regulatory landscape started to shape up.
Your Story
How’d you find your way into Vehicle Cybersecurity?

01 Existing automotive professional – career pivot

02 IT security folks lured into vehicle security

03 Government (FBI, CIA, etc.) pivot to industry

04 Car hacker/hobbyist turned professional

05 Academic
Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system

This document is meant purely as documentation tool. The authentic and legal binding text is: ECE/TRANS/WP.29/2020/79 (as amended by ECE/TRANS/WP.29/2020/94 and ECE/TRANS/WP.29/2020/97).
Automotive Security Research Group
The Origin

John Heldreth
• Master's Thesis
• August 2017: ASRG-Stuttgart First Meetup
October 2018: ASRG-Detroit First Meetup - Sean McKeever
ASRG

Why?

When you entered vehicle cybersecurity, don’t you wish…

• you had a community?
• you had resources?

When you were solving hard problems in vehicle cybersecurity, don’t you wish…

• you could refer to talks that might support you in solving it?
• you could talk to others from around the world to see how their perspective might shape your own?
• you could draw insight from people from completely different backgrounds - car hacker, academic, professional, etc.?
Sounds kind of like the Auto ISAC…

but it’s a focus on a different audience.
ASRG
Casting a much wider net
Losing people? Trying desperately to hire? Welcome to the club. If only there was a global pool of people that went out of their way to sign up with a non-profit in automotive security.

Passion and interest go a long way.
So, what’s the ASRG up to?
So what are we up to?: ASRG WORLD Webinars
So what are we up to?: ASRG Chapters

- Ideally, monthly in-person meetups led by a local chapter lead.
- Still trying to recover chapter events post-COVID
- Check out a chapter near you – they might be hosting an event. If not – ask them when the next one will be!
So what are we up to?: ASRG Academic Network

Solution

Technical Committees
Collaboration

Learning Platform
Knowledge

ASRG

Academic Societies
Networking

- Missing University Curriculums
- Inadequate Relationship to Industry
- Non-Applied Research
- No Certification Program
- High Barrier of Entry
ASRG

So what are we up to?: ASRG Projects & Technical Committees

• Automotive Security Intelligence Platform (ASIP)
  • garage.asrg.io/intelligence/
• Threat Catalog
  • garage.asrg.io/threat-catalog/
• Open Exchange for Security Analysis Models
  • openxsam.io
• Vulnerability Management
  • ASRG is a CVE Numbering Authority for automotive-applicable vulnerabilities
  • ASRG receives vulnerability disclosures
• EU Vehicle Security Operations Center
So what are we up to?: ASRG Secure Our Streets (SOS)

TOTAL REGISTERED
850

MAXIMUM PARTICIPANTS PER SESSION
282

AVERAGE PARTICIPANTS PER SESSION
116

TOP 10 DEMOGRAPHICS
- 33% | GERMANY
- 13% | INDIA
- 8% | UNITED STATES
- 8% | UNITED KINGDOM
- 7% | ISRAEL
- 3% | ROMANIA
- 2% | SPAIN
- 2% | SINGAPORE
- 2% | ITALY
- 2% | AUSTRIA

ROLES
- 63% | PROFESSIONAL
- 17% | RESEARCHER
- 7% | STUDENT
- 5% | STILL LOOKING FOR MYSELF...
- 2% | HOBBYIST / HACKER

#SecureOurStreets
Individuals: So how can you get involved?

Sign up at garage.asrg.io

- Join/start a local chapter.
- Contribute to an ASRG effort:
  - Lead a WORLD Webinar
  - Support a Project/Technical Committee
  - Support SOS
  - Support the Academic Network
- Join slack & stir up the conversation
  - [https://join.slack.com/t/asrg/shared_invite/zt-83ivvj85-Nny_0n8DN7HB1ws6w1u89g](https://join.slack.com/t/asrg/shared_invite/zt-83ivvj85-Nny_0n8DN7HB1ws6w1u89g)
ASRG

Companies: So how can you get involved?

**Supporter**
Supporters are individuals, corporations, or organizations contributing existing organizational resources to ASRG without risk. There is no official agreement/contract.
Example: Meeting Rooms, Tools, Garages, Educational Content, Presentations, etc.

**Sponsor**
A Sponsor is a formal agreement between an organization or corporation and ASRG. This formal agreement details the relationship, services and fixed donations.
Example: ASRG Marketing opportunities.
Defined Levels (see Slide)

**Partnership**
A Partnership is a formal agreement between a non-profit organization and ASRG to work together towards a common goal. Risks and benefits are shared based on the formal agreement.
Example: Other non-Profit organizations

Sponsorships index is changed every year because of new offerings from ASRG, and potential increase in donation requirements.
ASRG Toy Drive & Shop Talk

December 8th, 2022
@Block Harbor: 1111 Bellevue Street, Detroit, MI 48207
3-8pm

Topic: I’m a Vehicle Cybersecurity Expert, Change My Mind

#FILLTHEFRUNK

Food & Drink provided w/ a special guest visit
Admission: Free, but bring a toy or donate if you can
Questions / Comments
(Answers are also acceptable)
Any questions about the Auto-ISAC or future topics for discussion?
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 melissacromack@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).
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*

**Innovator**  
*Strategic Partnership (18)*
- ArmorText
- Cybellum
- Deloitte
- FEV
- GRIMM
- HackerOne
- Irdeto
- Itemis
- Karamba Security
- KELA
- Pen Testing Partners
- Red Balloon Security
- Regulus Cyber
- Saferide
- Security Scorecard
- Trustonic
- Upstream
- Vultara

**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 C51
- DHS HQ
- DOT-PIF
- FASTR
- FBI
- GAO
- ISAO
- Macon Business/MADCAT
- Merk (training, np)
- MITRE
- National White Collar Crime Center
- NCOFTA
- NDIA
- NHTSA
- NIST
- Northern California Regional Intelligence Center (NCRIC)
- NTIA - DoCommerce
- OASIS
- ODNI
- Ohio Turnpike & Infrastructure Commission
- SANS
- The University of Warwick
- TASA
- University of Tulsa
- USSC
- VOLPE
- W3C/MIT
- Walsh College

**Benefactor**  
*Sponsorship Partnership*
- 2022 Summit Sponsors-
  - Argus
  - BGNetworks
  - Bosch
  - Blackberry
  - Block Harbor
  - BlueVoyant
  - Booz Allen Hamilton
  - C2A
  - Cybellum
  - CyberGRX
  - Cyware
  - Deloitte
  - Denso
  - Finite State
  - Fortress
  - Itemis
  - Keysight Technologies
  - Micron
  - NXP
  - Okta
  - Sandia
  - Securonix
  - Tanium
  - UL
  - Upstream
  - VicOne

*Thanks for your Support to our Many Partners*

**Community Partners**
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