Welcome to Auto-ISAC!

Monthly Virtual Community Call

September 14, 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><img src="https://www.us-cert.gov/tlp" alt="Red" /></td>
<td>Not for disclosure, restricted to participants only.</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><img src="https://www.us-cert.gov/tlp" alt="Amber" /></td>
<td>Limited disclosure, restricted to participants organizations.</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><img src="https://www.us-cert.gov/tlp" alt="Green" /></td>
<td>Limited disclosure, restricted to the community.</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><img src="https://www.us-cert.gov/tlp" alt="White" /></td>
<td>Disclosure is not limited.</td>
<td></td>
</tr>
</tbody>
</table>

*From: https://www.us-cert.gov/tlp*
<table>
<thead>
<tr>
<th>Time (ET)</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>11:00</td>
<td><strong>Welcome</strong></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><strong>Auto-ISAC Update</strong></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>- What’s Trending</td>
</tr>
<tr>
<td>11:15</td>
<td><strong>DHS CISA Community Update</strong></td>
</tr>
<tr>
<td>11:20</td>
<td><strong>Featured Speaker:</strong></td>
</tr>
<tr>
<td></td>
<td>- Tim Weisenberger, Program Manager, SAE International</td>
</tr>
<tr>
<td></td>
<td>- Title: “SAE EV Charging Public Key Infrastructure Program”</td>
</tr>
<tr>
<td>11:45</td>
<td><strong>Around the Room</strong></td>
</tr>
<tr>
<td></td>
<td>- Sharing Around the Virtual Room</td>
</tr>
<tr>
<td>11:55</td>
<td><strong>Closing Remarks</strong></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)

**22** OEM Members

**21** Navigator Partners

**47** Supplier & Commercial Vehicle Members

**19** Innovator Partners

**Innovator Partners**

**Navigator Partners**

Engaging in the Auto-ISAC Community
### Member Roster
**As of September 2022**

<table>
<thead>
<tr>
<th>Company</th>
<th>Change</th>
<th>Members, Progress</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Aisin</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Allison Transmission</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>General Motors (Cruise-Affiliate)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Aptiv</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Geotab</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Argo AI, LLC</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Harman</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>AT&amp;T</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hitachi</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>AVL List GmbH</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Honda</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Blackberry Limited</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hyundai</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>BMW Group</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Infineon</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Borg Warner</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Intel</td>
<td></td>
<td></td>
</tr>
<tr>
<td>**Bosch (E Scrip Aff)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>John Deere Electronic</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Canoo</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Kia</td>
<td></td>
<td></td>
</tr>
<tr>
<td>**Continental (Argus Aff)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Knorr Bremse</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Cummins</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lear</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Denso</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LGE</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>e:fs</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lucid Motors</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Faurecia</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Luminar</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Flex</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Magna</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Ford</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MARELLI</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**As of September 2022**

- Members: 69
-待办事项: 8

**Eight Pending:** Thyssenkrupp; Cymotive; AAM, Ferrari, ChargePoint; Nuspire, KTM

---

**TLP: WHITE**
Upcoming Events

Upcoming Meetings

Community Call:
- Wednesday, October 5th – Speaker: TBA Title: “TBA” Time: 11 – 12:00 p.m. TLP:WHITE

European Workshop:
- Tuesday, October 11th, Working with Partners (Open to partners)
- Wednesday, October 12th, Automotive Scoring of Vulnerabilities and Vulnerability Monitoring (Members Only)

Announcements:

ACT Program Advanced Courses – Beta Advanced registration is open. Beta Advanced classes start September 19th. Contact Tamara Shoemaker.

NHTSA Updates Cybersecurity Best Practices for New Vehicles

CISA Releases its First Strategic Plan https://www.cisa.gov/strategy

CYBER INCIDENT REPORTING FOR CRITICAL INFRASTRUCTURE ACT OF 2022 (CIRCIA)
https://www.cisa.gov/circia
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 tension remains extremely high in and near Ukraine after the country’s recent counteroffensive against Russian occupation forces. Many Russian soldiers retreated to other parts of Ukraine in response but continue to monitor Russia’s actions/official statements today and in the coming days (Washington Post, PBS). Though unpredictable, the cyber threat Russia poses to global critical infrastructure should not be dismissed (CISA Shields Up, Trustwave, CISA-Technical Approaches to Uncovering and Remediating Malicious Activity).

  - Cybercriminal Groups Targeting Automotive: DESORDEN, RansomEXX, Black Basta.

  - Notable Incidents: Yandex Taxi app exploited (Hackread); Ransomware operators accessed UK water supplier’s industrial network via IT (Vice); NATO data stolen/leaked (BleepingComputer).

  - Notable Tactics Techniques and Procedures: multi-factor authentication bypass (The Stack, Microsoft, Engadget); exploiting open redirect vulnerabilities (Inky); intermittent encryption to evade detection (SentinelLabs); leveraging NTRUEncrypt public key encryption algorithm (BleepingComputer); backdooring Mimi app (The Hacker News); leveraging Dark Utilities C2aaS (Talos).
CISA RESOURCE HIGHLIGHTS
Stop Ransomware: Vice Society

Regardless of industry, service providers need to monitor threats.

The Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), and the Multi-State Information Sharing and Analysis Center (MS-ISAC) have released a joint CSA to disseminate IOCs and TTPs associated with Vice Society actors identified through FBI investigations as recently as September 2022.
CISA and the Multi-State Information Sharing & Analysis Center (MS-ISAC) published a joint Cybersecurity Advisory (CSA) in response to active exploitation of multiple Common Vulnerabilities and Exposures (CVEs) against Zimbra Collaboration Suite (ZCS), an enterprise cloud-hosted collaboration software and email platform.

CISA and the MS-ISAC recommend organizations upgrade to the latest ZCS releases as noted on Zimbra Security – News & Alerts and Zimbra Security Advisories.

- Adopt zero-trust principles and architecture
- Properly configure and secure internet-facing network devices.
- Ensure your organization has a vulnerability management program
The current geopolitical conflict has affected organizations all over the world, regardless of industry. Some of the greatest exploitations have resulted in financial, human resource, and other losses.

**CNMF has issued warnings.**

U.S. Cyber Command’s Cyber National Mission Force (CNMF), in close coordination with the Security Service of Ukraine, has released a list of indicators of compromise (IOCs) of malware seen in Ukraine. According to CNMF, “Ukrainian partners are actively sharing malicious activity they find with us to bolster collective cyber security, just as we are sharing with them.”

**We want to help you fight this vulnerability.**

CISA encourages users and administrators to review U.S. Cyber Command’s press release, Cyber National Mission Force discloses IOCs from Ukrainian networks, as well as their VirusTotal and GitHub pages for more information. See Mandiant’s report, Evacuation and Humanitarian Documents used to Spear Phish Ukrainian Entities, for additional information.

Read more here: CNMF Discloses Malware in Ukraine | CISA
CISA has added 23 new vulnerabilities to its Known Exploited Vulnerabilities Catalog in the month of August. 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
Featured Speaker
Tim Weisenberger manages SAE programs in emerging technology areas such as Vehicle Automation, Connectivity, Electrification, and Shared-use Mobility. Tim leads SAE’s cybersecurity portfolio and coordinates international standards collaboration and harmonization.
GLOBAL GROUND VEHICLE STANDARDS

Developing an EV Charging Public Key Infrastructure

an SAE Cooperative Research Project

Tim Weisenberger
Technical Program Manager
Emerging Technologies
SAE INTERNATIONAL
The Research Opportunity and How it Emerged...

EV Charging systems have crucial and growing interface points between the Automotive industry, EV drivers, and the Electric Grid/Energy industry.

- It is critical that these interfaces be **secure and trusted**

**Significant gaps in EV Charging PKI are hindering interoperability and security**

- ISO 15118 Plug N Charge Protocol Standard has PKI and cybersecurity elements, but is incomplete
- Only one PKI provider of a 15118-based PKI approach
- Industry and SAE formed a cooperative research project to create a modern, protocol-neutral industry PKI solution.
Project Approach and Goals

SAE Cooperative Research Program

SAE Cooperative Research Program (CRP) projects are partnerships of SAE and industry companies that meet project criteria to perform targeted, pre-competitive research to solve an industry problem.

SAE CRP projects develop industry deliverables that can then be fed into SAE standards to develop a needed J standard.

SAE EV Charging Public Key Infrastructure CRP

The project will design and test an inclusive, worldwide EV charging industry PKI platform that is secure, trusted, scalable, interoperable, and extensible.

The project is an industry-led, pre-competitive research project to strengthen electric vehicle charging system security.
### SAE EV Charging PKI Project Value to Industry

<table>
<thead>
<tr>
<th>Benefit</th>
<th>Feature</th>
<th>Value Add</th>
</tr>
</thead>
</table>
| **Lower Cost**                 | Platform operationalization by digital security services firm with demonstrated global experience | • Faster delivery of production & test certs  
• Lower risk of security breach  
• Disaster recovery & business continuity  
• Choice of CAs for issuance of certificates |
| **Increased Trust and Level of Security** | • Consortium acts as the Policy Authority (PA)  
• Full transparency of CAs and Registration Authority operations  
• Assurance the PKI is administered by subscribers and new CAs according to CP and CPS | • Robust, cradle-to-grave certificate life-cycle mgmt.  
• Out-of-band operations eliminated  
• Response robustness in disaster scenario |
| **More Control**               | PA determines if & when PKI changes are needed due to industry regulations, governance, technical, or operational reasons | • Enforce conformance to CPS  
• Manage on-boarding of CAs, Trust Lists, ICAs, etc. |
**Project Overview**

**Core Project Team**
- ChargePoint
- eMobility Power
- Electrify America
- Ford
- General Motors
- MBRDNA (Daimler)
- Rivian
- Shell
- Stellantis

**Technical Development**
Core Team is technical lead; Technical work performed by paid technical Contractors Eonti and DigiCert; SAE International is administrative PM
- **PKI Platform Design complete**
- Testing underway
- Project Close-out in Q4

**Migration Path**
SAE and Core Team will migrate the technical project to an operational industry EV Charging PKI Enterprise
Technical Deliverables

Phase 1 Design Complete
- PKI Design and Prototype
- Operationalization Planning Report

*SAE EV Charging PKI Platform compatibility with ISO/IEC 15118-2 is built-in and pre-tested.*

Phase 2 Testing
Friendly Platform functionality and scalability testing with project members
- Virtual Testing Platform
- Testing at NREL in Golden, CO Apr 4-7, 2022 and Sep 12-16, 2022
- Adversarial Testing performed by Sandia Labs

Migration Path

Consortium Planning Group
Participants will meet to plan the governance and operations of an industry Consortium.
- *Separate activity from the CRP; will meet in the SAE Industry Technologies Consortia*

Maintain Virtual PKI Testing Platform
- Further engagement of industry; additional test events in 2023 (TBD)

EV Charging PKI Industry Consortium
Launch an EV Charging PKI consortium to field an industry EV Charging PKI enterprise
Completed Project Deliverables

Completed Design Deliverables

Industry Review and Gap Analysis

Threat Model

PKI Platform Design Package

- PKI Requirements Doc (PRD)
- PKI Prototype
- Certificate Policy

Operationalization Report
SAE EV Charging PKI “Friendly” Test Event; April 4, 2022

What was tested?

- Issuance of certificates to participants from a cloud-based CA platform via a central RA and APIs
- The EV to EVSE interface using compliant certificates with 256-bit ECC keys
- TLS and PnC with ISO 15118-2 compliant EVs and EVSEs
- Sending non-compliant EV certificates to the EVSE

Was the testing a success?

Yes, the test demonstrated the compliance and interoperability of the certificates such that:

- An EV performed TLS and PnC with two different EVSEs; and
- An EVSE performed TLS and PnC with two different EVs

What did we learn from the test event?

More testing is needed, ideally with additional EV and EVSEs, as well as the backend CPO/MO application to provide the needed data to develop the certificate validation policy.
Expanded Friendly Test; Sep 12-16, 2022

Testing Expanded and Refined:
• Test interface between EVSE and CPO/MO, Certificate Revocation, non-compliant EVSE certificates to EVs, and certificates with 521-bit ECC keys
• More Robust Interoperability Testing- 3 EVs, 6 Chargers, 2 Charging Back-ends

Adversarial testing
• Sandia National Lab to perform ethical hacking event of the EV to EVSE interface

Further modularization
• self-testing documentation
• operational user guidelines
• repository of certs
• demo/test examples
• APIs
• past testing reports
SAE EV Charging PKI Migration Path

Consortium Planning Group
Participants will meet to plan the governance and operations of an industry Consortium.

• Separate activity from the CRP; will meet in the SAE Industry Technologies Consortia

Maintain Virtual PKI Testing Platform

• Further engagement of industry for testing
• Additional test events in 2023 (TBD)

EV Charging PKI Industry Consortium
Launch an EV Charging PKI consortium to field an industry EV Charging PKI enterprise
SAE EV Charging PKI Project Migration to EV Charging Industry PKI

1. **Project Core Team**
   - Paid Technical Performer

**Technical Deliverables:**
1. EV Charging PKI Platform
2. Handover Plan to field an Industry PKI

2. **Virtual PKI testing Platform**
   - Virtual PKI testing support and maintenance (Outside scope of CRP)

3. **Consortium Planning**
   - (Parallel Activity to CRP)

- **EV Charging Industry PKI Consortium**
  - PKI Policy Authority

- **Operational PKI**
  - Procurement(s)
  - CA, RA, Certification Testing, Threat Monitoring, etc.

Future publication of SAE EV Charging PKI Platform Documents TBD during the migration to a consortium and operational industry PKI entity.

**Timeline:**
- **Jan 2021**
  - Design Complete
- **Dec 2021**
  - Test Event 1
- **Apr 2022**
  - Test Event 2
- **Sep 2022**
  - Test Event 2
- **Oct 2022**
  - Project Complete
- **Q4 2022/2023**
- **FY2023**
Come Join Us!

Please contact Tim Weisenberger to engage in the SAE EV Charging PKI CRP.

Tim Weisenberger
Technical Program Manager, Emerging Technologies

e: tim.weisenberger@sae.org
m: 248.840.2106
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!

How to Get Involved: Membership

➢ 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 michaelshokouhi@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

Thanks for your Support to our Many Partners

Community Partners

INNOVATOR
Strategic Partnership
(19)
- ArmorText
- Cybellum
- Deloitte
- FEV
- GRIMM
- HackerOne
- Irdeto
- Itemis
- Karamba Security
- KELA
- Pen Testing Partners
- Red Balloon Security
- Regulus Cyber
- Saferide
- Security Scorecard
- Tanium
- 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
- Comteest
- Cyber Truck Challenge
- DHS CSVI
- DHS HQ
- DOT-PIF
- FASTR
- FBI
- GAO
- ISAO
- McAmb Business/MADCAT
- Merk (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
- USCC
- VOLPE
- W3C/MIT
- Walsh College

BENEFACTOR
Sponsorship Partnership
2021 Summit Sponsors-
- Celerium
- Cyware
- Denso
- NDIA
- IOActive
- Claroty
- Deloitte
- Finite State
- Tanium
- Recorded Future
- PaloAlto Networks
- Upstream
- Securonic
- Zimperium
- Micron
- Block Harbor
- SecurityScorecard
- Booz Allen
- CybelAngel
- ATT
- Ford
- Cybellum

2020 Summit Sponsors-
- Claroty
- Upstream
- Encrypt
- Blackberry
- Cybellum
- Blockharbor
- C2A
- Synopsis
- Intsights
- ValiMail

TLP:WHITE
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
## Our Contact Info

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
<th>Address</th>
<th>Phone</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Faye Francy</td>
<td>Executive Director</td>
<td>20 F Street NW, Suite 700</td>
<td>703-861-5417</td>
<td><a href="mailto:fayefrancy@automotiveisac.com">fayefrancy@automotiveisac.com</a></td>
</tr>
<tr>
<td>Sharmila Khadka</td>
<td>Information Technology Executive Coordinator</td>
<td>20 F Street NW, Suite 700</td>
<td>443-962-5663</td>
<td><a href="mailto:sharmilakhadka@automotiveisac.com">sharmilakhadka@automotiveisac.com</a></td>
</tr>
</tbody>
</table>

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