



WELCOME TO AUTO-ISAC!

MONTHLY VIRTUAL COMMUNITY CALL





January 5, 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">▪ Paul Eisler, <i>Senior Director of Cybersecurity, USTelecom</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*

15
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



Alan Houck
Chair of the SAG
NXP



Larry Hilken
Chair of the CAG
Cummins

MEMBER ROSTER

AS OF JANUARY 2022

64 Members, 1 in Progress

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

BUSINESS ADMINISTRATION

➤ Analyst Working Group (AWG):

- **Tuesday, January 11 - Agenda:** No presenter currently scheduled; **RED** Platform Discussion; Hot Topics Discussion; **Time:** 10 – 11:30 a.m. ET **MEMBER ONLY.**

➤ Upcoming Key Events:

➤ Community Call:

- **Wednesday, February 2 - Speaker:** Victor Murray, SWRI **Title:** *Research into Defending Automobiles via Intrusion Detection Systems (IDS)* **Time:** 11 – 12:00 p.m. **TLP:WHITE**

➤ Announcements:

- **Auto-ISAC & NHTSA's Automotive Cybersecurity Training (ACT)** launches with the first set of classes on January 10. **MEMBER ONLY.**
- **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](#).
- **SAG's SBoM Working Group** is finalizing their proposed **SBoM Best Practice Guide**. A Meeting will be scheduled for mid-January during which time the SBoM WG will present the guide and their plan for review and approval by the Board.
- **Auto-ISAC Annual Report:** In work for BoD Review/Approval in Q1 '22



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 this quarter.
- Intelligence Notes
 - Open-source reporting about the Log4j vulnerability (Log4Shell) has begun to subside but **the threat will linger for the foreseeable future**. IT, OT, and product cybersecurity teams should be on lookout for and study credible reports of cyber incidents involving Log4Shell, assess whether your organization is at risk of similar attacks, and carefully implement countermeasures as appropriate ([CISA](#), [Microsoft](#), [GitHub NCSC-NL](#)).
 - Cybersecurity teams should proactively **imagine** (red team) ways Log4Shell could be exploited to compromise your networks, systems, and products. Assume sophisticated threat actors are patiently seeking ways to exploit the vulnerability even if more elaborate attack chains are necessary.
 - Cybersecurity teams should monitor geopolitical developments regarding ongoing tensions between Russia and Ukraine as **such tension could yield cyberattacks that cause adverse spillover impacts to environments worldwide** ([The Hill](#), [CBC](#), [GovInfoSecurity](#)).

CISA RESOURCE HIGHLIGHTS



TLP: WHITE – Eighteen (18) Known Exploited Vulnerabilities Added to the KEV Catalog in December 2021 Resources

- **The following CISA Current Activities (CAs) provide tables of the KEVs that were added:**
 - [https://www\[.\]cisa\[.\]gov/uscert/ncas/current-activity/2021/12/10/cisa-adds-thirteen-known-exploited-vulnerabilities-catalog](https://www[.]cisa[.]gov/uscert/ncas/current-activity/2021/12/10/cisa-adds-thirteen-known-exploited-vulnerabilities-catalog)
 - [https://www\[.\]cisa\[.\]gov/uscert/ncas/current-activity/2021/12/01/cisa-adds-five-known-exploited-vulnerabilities-catalog](https://www[.]cisa[.]gov/uscert/ncas/current-activity/2021/12/01/cisa-adds-five-known-exploited-vulnerabilities-catalog)
- **KEV Catalog:**
 - [https://www\[.\]cisa\[.\]gov/known-exploited-vulnerabilities-catalog](https://www[.]cisa[.]gov/known-exploited-vulnerabilities-catalog)



TLP: WHITE – CISA Current Activities (CA) – Apache Log4j Vulnerability Resources

- **CISA ED 22-02 Directing Federal Agencies to Mitigate Apache Log4j Vulnerabilities**
 - [https://www\[.\]cisa\[.\]gov/uscert/ncas/current-activity/2021/12/17/cisa-issues-ed-22-02-directing-federal-agencies-mitigate-apache](https://www[.]cisa[.]gov/uscert/ncas/current-activity/2021/12/17/cisa-issues-ed-22-02-directing-federal-agencies-mitigate-apache)
 - [https://www\[.\]cisa\[.\]gov/emergency-directive-22-02](https://www[.]cisa[.]gov/emergency-directive-22-02)
- **CISA's Apache Log4j Vulnerability Guidance webpage**
 - [https://www\[.\]cisa\[.\]gov/uscert/apache-log4j-vulnerability-guidance](https://www[.]cisa[.]gov/uscert/apache-log4j-vulnerability-guidance)



TLP: WHITE – CISA Current Activity (CA) – CISA and FBI Release Alert on Active Exploitation of CVE-2021-44077 in Zoho ManageEngine ServiceDesk Plus

- CISA and the FBI published joint Cybersecurity Advisory AA21-336A, identifying active exploitation of CVE-2021-44077—in Zoho ManageEngine ServiceDesk Plus.
- AA21-336 includes a list of tactics, techniques and procedures, including the ATT@CK framework references, used to exploit CVE-2021-44077
- See:
 - [https://www\[.\]cisa\[.\]gov/uscert/ncas/current-activity/2021/12/02/cisa-and-fbi-release-alert-active-exploitation-cve-2021-44077-zoho](https://www[.]cisa[.]gov/uscert/ncas/current-activity/2021/12/02/cisa-and-fbi-release-alert-active-exploitation-cve-2021-44077-zoho)
 - [https://us-cert\[.\]cisa\[.\]gov/ncas/alerts/aa21-336a](https://us-cert[.]cisa[.]gov/ncas/alerts/aa21-336a)



TLP: WHITE – CISA Current Activities (CA) – Immediate Steps to Strengthen Critical Infrastructure against Potential Cyberattacks

- **CISA Insights: Preparing For and Mitigating Potential Cyber Threats** provides critical infrastructure leaders with steps to proactively strengthen their organization’s operational resiliency against sophisticated threat actors, including nation-states and their proxies
- **Resources at:**
 - [https://www\[.\]cisa\[.\]gov/uscert/ncas/current-activity/2021/12/15/immediate-steps-strengthen-critical-infrastructure-against](https://www[.]cisa[.]gov/uscert/ncas/current-activity/2021/12/15/immediate-steps-strengthen-critical-infrastructure-against)
 - [https://www\[.\]cisa\[.\]gov/publication/preparing-and-mitigating-potential-cyber-threats](https://www[.]cisa[.]gov/publication/preparing-and-mitigating-potential-cyber-threats)



TLP: WHITE – CISA Capacity Enhancement Guides (CEGs) Protecting Organization-Run Social Media Accounts

- Actionable measures described in the CEG aim to reduce the risk of unauthorized access on platforms such as Twitter, Facebook, and Instagram.
- Details available at:
 - [https://www\[.\]cisa\[.\]gov/uscert/ncas/current-activity/2021/12/09/cisa-releases-guidance-protecting-organization-run-social-media](https://www[.]cisa[.]gov/uscert/ncas/current-activity/2021/12/09/cisa-releases-guidance-protecting-organization-run-social-media)
 - [https://www\[.\]cisa\[.\]gov/capacity-enhancement-guides-federal-agencies](https://www[.]cisa[.]gov/capacity-enhancement-guides-federal-agencies)



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 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/)
- CISA COVID-19 Response – [https://www\[.\]cisa\[.\]gov/coronavirus](https://www[.]cisa[.]gov/coronavirus)
- CISA Webinar Series on YouTube: [https://www\[.\]youtube\[.\]com/playlist?list=PL-BF3N9rHBLJN3HUIZnTnyZHex9gPk_Yy](https://www[.]youtube[.]com/playlist?list=PL-BF3N9rHBLJN3HUIZnTnyZHex9gPk_Yy)





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

Questions?
CISAServiceDesk@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



PAUL EISLER- USTELECOM

SENIOR DIRECTOR OF CYBERSECURITY



Paul Eisler is the Senior Director of Cybersecurity at USTelecom. An attorney with more than a decade of experience in cyber policy, he serves on the Secretariat of the Council to Secure the Digital Economy (CSDE), a partnership of 15 global ICT companies that publish influential security guidance, and he co-chairs the Cybersecurity Committee of the Communications Sector Coordinating Council (CSCC), which facilitates public-private cyber initiatives across the U.S. government.

Since CSDE's founding, Paul has been the principal editor of the CSDE International Botnet and IoT Security Guide, published annually, and he led the effort to develop the CSDE IoT Security Policy Principles, endorsed by 27 major ICT organizations. His research on IoT practices laid the groundwork for the C2 Consensus on IoT Device Security Baseline Capabilities, endorsed by 20 major ICT organizations including standards bodies.

He received his law degree with honors from American University Washington College of Law, where he served on the American University Law Review and, at age 20, was distinguished as the law school's youngest J.D. candidate. He also worked for his alma mater as a Legal Research Fellow, concentrating on economic policies of the European Union.

CYBER CRISIS RESPONSE AND HANDLING



Leading the Fight Against Cyber Threats

- To protect our digital ecosystem, industry's dedication to security must equal its passion for innovation.
- Led by **USTelecom** and **CTA**, the Council to Secure the Digital Economy (CSDE) is comprised of these members:
 - Akamai
 - AT&T
 - Cisco
 - Ericsson
 - IBM
 - Intel Corporation
 - Lumen
 - NEC
 - NTT
 - Oracle
 - Panasonic
 - Samsung
 - SAP
 - Telefónica
 - Verizon



What Keeps Us Up at Night?

- ▶ A CYBER CRISIS is a real possibility
- ▶ ICT sector's readiness, speed and capabilities are paramount
- ▶ We have seen cyber-attacks against:
 - power plants
 - oil and gas companies
 - financial centers
 - military organizations
 - hospitals
 - governments
 - virtually every other sector
- ▶ Threat actors evolving techniques, tactics, and procedures (TTPs)
- ▶ Log4j has triggered highest levels of concern



Who You Gonna Call?

- ▶ Individual company VS multi-party coordination
- ▶ Confirmed incidents VS vulnerability handling
- ▶ Crisis planning to build capacity and “muscle memory”
- ▶ Best practices and standards
- ▶ Collaboration with USG (e.g., CISA’s JCDC)



Roles in Crisis Response

- ▶ CSDE's [Cyber Crisis Report](#) available at CSDE.org

- ▶ Examines 12 potential crisis scenarios:
 - *DDoS Botnet Attack*
 - *DDoS Server-based Attack*
 - *Border Gateway Protocol (BGP) Hijacking*
 - *Domain Name System (DNS) Hijacking*
 - *Software Vulnerabilities: Open Source*
 - *Software Vulnerabilities: Zero Day*
 - *Hardware Vulnerabilities: Processor Architectures*
 - *Injection of Malicious Code in Software and Hardware Components*
 - *Destructive Malware*
 - *Ransomware*
 - *Advanced Persistent Threat (APT): Industrial Systems*
 - *Cloud Provider Compromise*



Key Insights

- ▶ Share knowledge of threats and confirmed incidents
- ▶ Build close government-industry working relationships
- ▶ Collaborate to address vulnerabilities
- ▶ Keep sensitive info confidential, until a remediation is available **and publicly released**
- ▶ Mobilize rapidly when an incident occurs
- ▶ Enhance international cooperation



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 Partner

Solutions Providers

For-profit companies that sell connected vehicle cybersecurity products & services.

Examples: Hacker ONE, IOActive, Karamba, Grimm

INNOVATOR
Paid Partnership

- Annual investment and agreement
- Specific commitment to engage with ISAC
- In-kind contributions allowed
- Must be educational provide awareness

Community Partners

Associations

Industry associations and others that want to support and invest in the Auto-ISAC activities.

Examples: Auto Alliance, ATA, ACEA, JAMA

NAVIGATOR
Support Partnership

- Provides guidance and support
- Annual definition of activity commitments and expected outcomes
- Provides guidance on key topics / activities
- Supports Auto-ISAC

Affiliations

Government, academia, research, non-profit orgs with complementary missions to Auto-ISAC.

Examples: NCI, DHS, NHTSA, Colorado State

COLLABORATOR
Coordination Partnership

- “See something, say something”
- May not require a formal agreement
- Information exchanges-coordination activities
- Information Sharing / research & development

Community

Companies or individuals interested in engaging the automotive ecosystem and supporting & educating the community.

Examples: Sponsors for key events, technical experts, etc.

BENEFACTOR
Sponsorship Partnership

- Participate in monthly community calls
- Sponsor Summit
- Network with Auto Community
- Webinar / Events

CURRENT PARTNERSHIPS

MANY ORGANIZATIONS ENGAGING

INNOVATOR

**Strategic Partnership
(15)**

ArmorText
Celerium
Cybellum
Ernst and Young
FEV
GRIMM
HackerOne
Karamba Security
Pen Testing Partners
Red Balloon Security
Regulus Cyber
Saferide
Security Scorecard
Trillium Secure
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**

2020 Summit Sponsors-

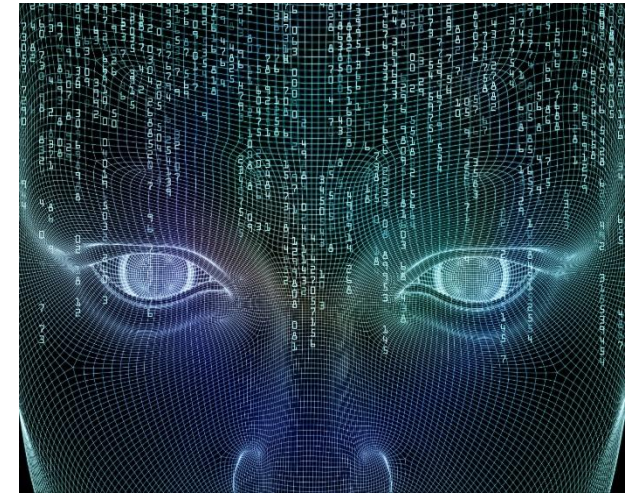
Claroty
Upstream
Escrypt
Blackberry
Cybellum
Blockharbor
C2A
Synopsis
Intsignts
ValiMail

2019 Summit Sponsors-

Argus
Arxan
Blackberry
Booz Allen Hamilton
Bugcrowd
Celerium
Cyber Future Foundation
Deloitte
GM
HackerOne
Harman
IOActive
Karamba Security
Keysight
Micron
NXP
PACCAR
Recorded Future
Red Balloon Security
Saferide
Symantec
Toyota
Transmit Security
Upstream
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

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)