



WELCOME TO AUTO-ISAC!





MONTHLY VIRTUAL COMMUNITY CALL

August 4, 2021

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">▪ Suzanne Lightman, <i>Sr. Advisor Information Security, NIST</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

41 *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)*



2021 BOARD OF DIRECTORS

EXECUTIVE COMMITTEE (EXCOM)



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



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



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



Todd Lawless
*Chair of the
Advisory Board*
Continental



Michael Feiri
*Vice Chair of the
Advisory Board*
ZF



Chris Lupini
Chair of the SAG
Aptiv



Larry Hilkene
Chair of the CAG
Cummins

2021 ADVISORY BOARD (AB) LEADERSHIP

MEMBER ROSTER

AS OF AUGUST 1, 2021

63 Members

Aisin	Hyundai	NXP
Allison Transmission	Infineon	Oshkosh Corp
Aptiv	Intel	PACCAR
Argo AI, LLC	John Deere Electronic	Panasonic
AT&T	Kia	Polaris
Blackberry Limited	Knorr Bremse	Qualcomm
BMW Group	Lear	Renesas Electronics
BorgWarner	LGE	Stellantis
Bosch (Escrypt-Affiliate)	Luminar	Subaru
Continental (Argus-Affiliate)	Magna	Sumitomo Electric
Cummins	MARELLI	Tokai Rika
Denso	Mazda	Toyota
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

BUSINESS ADMINISTRATION

➤ Members ONLY Activities: TLP:AMBER

- **Auto-ISAC Members Teaching Members:** Wednesday, August 18, 2021, 10-11:30 am ET
 - Charles Wilson, *Principal Engineer, Cybersecurity Development Lifecycle Practice, Motional*
 - Presentation Title: “*Autonomous Vehicle Cybersecurity Development Lifecycle (AVCDL)*”

➤ Community Activities: TLP: GREEN

- **Community Call Speaker:** Wednesday, September 1st, 2021, 11-12 pm ET
 - Ms. Kayle Giroud, *Partnership Associate Director , GCA*; Ms. Gill Thomas, *Director of Engagement, Capacity & Resilience Program, GCA*
 - Presentation Title: “*Introduction to the Global Cyber Alliance (GCA)*”
- **Auto-ISAC Mid-year Community Call Survey:** COMPLETE

➤ Auto-ISAC Annual Cybersecurity Summit: TLP:WHITE

- Hybrid, October 13-14, 2021, 8:00 am – 5:00 pm
- GM Titanium Sponsor at RenCen, Detroit, MI
- REGISTER!!!



AUTO-ISAC CYBERSECURITY SUMMIT | OCT 13-14TH | HYBRID



**Event Host
Titanium Sponsor**

TAKE → CHARGE

SUMMIT
Oct. 13-14,
2021
Detroit | Virtual

Registration Open || Agenda & Themes on Website || Sponsor Prospectus on Website



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
- Know our strategic perception of and outlook for the cyber threat environment by reading the 2020 Threat Assessment in the Auto-ISAC 2020 Annual Report. The 2021 Annual Report and Threat Assessment are in production
 - Email us to request the report, provide feedback, or ask questions
- **Intelligence Notes**
 - Application programming interfaces (APIs) are increasingly being targeted as new vulnerabilities continue to be found ([BleepingComputer](#), [BleepingComputer](#), [Cyware](#), [ZDNet](#)).
 - APIs are predicted to become “the most frequent attack vector by 2022.” ([Gartner](#)).
 - Expanded use of APIs is a feature of digital transformation across industries ([Security Boulevard](#)).
 - Open-source API security best practices to consider ([Outpost24](#), [TechBeacon](#)).

AUTO-ISAC INTELLIGENCE

➤ Intelligence Notes Continued...

- The market for Initial Access Brokers is expanding, creating incentives for threat actors to focus their efforts on one critical step in the attack chain – initial access ([ZDNet](#), [Recorded Future](#)).
- This division of labor could increase cyber threats facing major industries including automotive as groups of threat actors spend focused time and energy on gaining initial access to vulnerable networks (while also likely honing their skills through experience).
- Maintain awareness of penetration testing tools (e.g., Cobalt Strike) that: (1) anyone, especially threat actors, can obtain legally or illegally and (2) can be used to infiltrate, disrupt, and/or damage your products or infrastructure.
- Notable Sources: [TechRepublic](#), [BleepingComputer](#), [BleepingComputer](#)

CISA RESOURCE HIGHLIGHTS



TLP: WHITE – CISA Industrial Control Systems Joint Working Group (ICSJWG) Fall Virtual Meeting – 20-21 September 2021

- **Summary for the Fall ICSJWG, an event flyer and resources from past ICSJWG meetings are available at [https://us-cert\[.\]cisa\[.\]gov/ics/icsjwg-meetings-and-webinars](https://us-cert[.]cisa[.]gov/ics/icsjwg-meetings-and-webinars)**
- **Registration link for the event will be made available at [https://cisa\[.\]gov/icsjwg](https://cisa[.]gov/icsjwg)**
- **Contact the ICSJWG team at [ICSJWG.Communications@cisa\[.\]dhs\[.\]gov](mailto:ICSJWG.Communications@cisa[.]dhs[.]gov) for more information**



TLP: WHITE – CISA Current Activity (CA) – CISA Announces Vulnerability Disclosure Policy (VDP) Platform

- **Single, centrally managed website that agencies can leverage as the primary point of entry for intaking, triaging, and routing vulnerabilities disclosed by researchers**
- **Allows agencies to gain greater insights into potential vulnerabilities, which will improve their cybersecurity posture**
- **Additional details at:**
 - [https://us-cert\[.\]cisa\[.\]gov/ncas/current-activity/2021/07/30/cisa-announces-vulnerability-disclosure-policy-vdp-platform](https://us-cert[.]cisa[.]gov/ncas/current-activity/2021/07/30/cisa-announces-vulnerability-disclosure-policy-vdp-platform)
 - [https://www\[.\]cisa\[.\]gov/blog/2021/07/29/cisa-announces-new-vulnerability-disclosure-policy-vdp-platform](https://www[.]cisa[.]gov/blog/2021/07/29/cisa-announces-new-vulnerability-disclosure-policy-vdp-platform)



TLP: WHITE – CISA CA – Joint Cybersecurity Advisory – Top Routinely Exploited Vulnerabilities

- Cooperative effort by CISA, FBI, Australian Cybersecurity Centre (ACSC), UK National Cybersecurity Centre (NCSC).
- Details the top vulnerabilities routinely exploited by malicious actors in 2020 and those being widely exploited thus far in 2021
- Resources:
 - [https://us-cert\[.\]cisa\[.\]gov/ncas/current-activity/2021/06/30/printnightmare-critical-windows-print-spooler-vulnerability](https://us-cert[.]cisa[.]gov/ncas/current-activity/2021/06/30/printnightmare-critical-windows-print-spooler-vulnerability)
 - [https://us-cert\[.\]cisa\[.\]gov/ncas/current-activity/2021/07/06/microsoft-releases-out-band-security-updates-printnightmare](https://us-cert[.]cisa[.]gov/ncas/current-activity/2021/07/06/microsoft-releases-out-band-security-updates-printnightmare)



TLP: WHITE – CISA CA - NSA Releases Guidance on Securing Wireless Devices While in Public

- Valuable guidance to the general public, with focus on users in the National Security System (NSS), Department of Defense (DoD), and Defense Industrial Base (DIB) communities
- The guidance also provides information on malicious techniques used by cyber actors to target wireless devices and ways to protect against it
- See:
 - [https://us-cert\[.\]cisa\[.\]gov/ncas/current-activity/2021/07/30/nsa-releases-guidance-securing-wireless-devices-while-public](https://us-cert[.]cisa[.]gov/ncas/current-activity/2021/07/30/nsa-releases-guidance-securing-wireless-devices-while-public)
 - https://media.defense.gov/2021/Jul/29/2002815141/-1/-1/0/CSI_SECURING_WIRELESS_DEVICES_IN_PUBLIC.PDF



TLP:WHITE – CISA CA – 2021 CWE Top 25 Most Dangerous Software Weaknesses

- Released by the Homeland Security Systems Engineering and Development Institute (HSSEDI), and operated by MITRE
- CWE uses data from the National Vulnerability Database (NVD) to compile the most frequent and critical errors that can lead to serious vulnerabilities in software
- See:
 - [https://us-cert\[.\]cisa\[.\]gov/ncas/current-activity/2021/07/21/2021-cwe-top-25-most-dangerous-software-weaknesses](https://us-cert[.]cisa[.]gov/ncas/current-activity/2021/07/21/2021-cwe-top-25-most-dangerous-software-weaknesses)
 - [https://cwe\[.\]mitre\[.\]org/top25/archive/2021/2021_cwe_top25.html](https://cwe[.]mitre[.]org/top25/archive/2021/2021_cwe_top25.html)



TLP: WHITE – Additional Resources From CISA

- CISA Homepage - [https://www\[.\]cisa\[.\]gov/](https://www[.]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 Vulnerability Management (formerly known as the National Cyber Assessment and Technical Services (NCATS) program) - [https://www\[.\]us-cert\[.\]gov/resources/ncats/](https://www[.]us-cert[.]gov/resources/ncats/)
- 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)





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



SUZANNE LIGHTMAN, NIST

SENIOR ADVISOR- INFORMATION SECURITY



Suzanne Lightman is a Senior Advisor at the Computer Security Division of the Information Technology Lab at the National Institute of Standards and Technology (NIST). In that position, she serves as the main point for cybersecurity and transportation systems as well as of industrial systems.

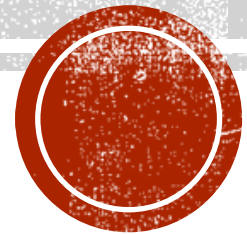
She has been involved in a diverse topics including development of the Cybersecurity Framework required under Executive Order 13636, cybersecurity in cyber-physical systems, identity management, IoT cybersecurity and cybersecurity & privacy policy. Her standards work includes automotive cybersecurity engineering (SAE/ISO 21434) & industrial cybersecurity (IEC 62443).

Ms. Lightman has two decades of experience in cybersecurity policy and implementation in positions all over the government, as well as in the private sector. She has held positions in both the legislative and executive branches which gives her a unique perspective on the development and implementation of government policy. In addition, she has worked on ethical hacking teams as well as led in-depth audits and reviews of cybersecurity.

CYBERSECURITY STANDARDS OVERVIEW FOR AUTO-ISAC

Suzanne Lightman

NIST



TOPICS

- Brief overview of cybersecurity standards work
- Automotive specific work
 - Joint SAE/ISO
 - SAE
 - ISO TC22
 - IEEE
 - UNECE
- Work that may be impactful
 - ISO
 - U.S. Government
- Getting involved



SHORT INTRODUCTION TO NIST

- Working with industry and science to advance innovation and improve quality of life.
- A few of our topics:



Artificial
Intelligence



Quantum
Science



Manufacturing



Cybersecurity



STANDARDS OVERVIEW

- Standards are
 - What should exist
 - Based on consensus
 - Technology neutral
 - Written for experts
- Standards are not
 - How to do something
 - Dependent on specific technological solutions
 - Biased to a particular viewpoint within an industry (i.e., a specific approach by one company)
 - Mandatory



MAJOR STANDARD DEVELOPMENT ORGANIZATIONS

- Specifically focused on automotive cybersecurity
 - SAE/ISO JWG
 - SAE
 - ISO – TC 22
 - IEEE/Uptane
 - UNECE WP.29
- Working on automotive cybersecurity adjacent topics
 - ISO JTC-1
 - ISA 99/IEC 65
- Other interesting groups
 - IIC
 - NMFTA



AUTOMOTIVE SPECIFIC WORK - JWG

- ISO/SAE JWG
 - 21434
 - Passed voting on final draft international standard
 - Should be issued by the fall
 - Do you really need a primer on this one?
 - Future work
 - Cybersecurity assurance levels/target attack feasibility (CAL and TAF)
 - Risk assessment scales
 - Standards harmonization



AUTOMOTIVE WORK - SAE

- TeeVee 18A cybersecurity
 - SAE side of the JWG
 - Verification and validation under 21434
 - Methodologies
 - Maturity model for automotive cybersecurity
 - Possible path for a certification program
- Data connector
 - Close to issuing a standard



AUTOMOTIVE WORK – ISO TC22

- **TC22/SC32**
 - **WG11 Cybersecurity**
 - ISO side of the JWG
 - Harmonization
 - Verification and validation
 - CAL/TAF
 - Audit
 - **WG12 Updates**
 - Passed CD stage
 - DIS due for ballot in the fall
 - **WG13 Safety for driving automation systems**
 - Working on developing a specification for assessing safety
 - Has cybersecurity as part of that



AUTOMOTIVE WORK IN IEEE

- IEEE is now the home of Uptane
 - Open and secure software update design for automotive
 - IEEE-ISTO 1600.1.0.0
- IEEE has too many cybersecurity activities to mention
 - However, they have excellent publications which I recommend for technical information



UNECE AUTOMOTIVE WORK

- **CS/OTA Informal Working Group on Over the Air Updates**
 - Issued a draft requirement under the 1998 agreement
 - Up for vote in September by the GVRA
 - If approved, may go to WP.29 in March
 - May not be deemed necessary
 - Recommended guidelines
 - Not a global technical regulation
 - May be adopted by regulatory authorities
- **Some other informal working groups**
 - Functional requirements for autonomous vehicles
 - Validation methods
 - ADAS



INTERESTING WORK IN JTC-1

- JTC-1/SC-27
 - Joint committee between ISO, IEEE and IEC to coordinate work in the IT arena
 - SC27's topic is cybersecurity
 - Working groups on
 - Privacy
 - Cryptography
 - Identity management
 - Information security management systems (ISO 27000 series)
 - Security evaluation, testing and specification
 - Security controls and services
 - And on and on
 - New working group (WG13) on trustworthiness has been established



INTERESTING WORK IN OTHER AREAS

- **NMFTA**
 - Non-standard but a locus of knowledge on cybersecurity focusing on the heavy-duty truck space
- **ISA99 and IEC 65**
 - Authoring committee for ISA/IEC 62443 standard on cybersecurity for industrial systems
 - Well-established standard for manufacturing
 - Mentioned in 21434
- **G-32**
 - SAE committee
 - Focusing on cyber-physical systems and cybersecurity
- **IIC**
 - Work on IoT and cloud



US GOVERNMENT WORK

- Department of Energy
 - New version of C2M2 just released
 - Cybersecurity Capability Maturity Model
 - Aimed originally at the power industry but now in much wider use
- NIST
 - Intent to revise SP 800-82 on cybersecurity of industrial systems
 - Publication of SP 800-53 rev5 imminent
 - Published definition of 'critical software'
 - Work on cybersecurity of positioning, navigation and timing
- DHS/CISA
 - Working on EO on Improving the Nation's Cybersecurity
 - Ransomware

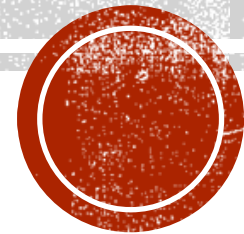


HOW TO GET INVOLVED

- **SAE**
 - If you are a member of SAE, you can join a committee and participate as an expert on their work
 - Global membership
 - SAE functions as the US TAG (Technical Advisory Group) to ISO TC22
- **ISO**
 - Participation in ISO work is through national bodies represented by TAGs
 - You would need to identify the group in your nation which functions as the TAG
 - You then ask to join the TAG for the working group you are interested in
 - **IEEE**
 - Membership is individual and members can participate in committees



QUESTIONS?



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-

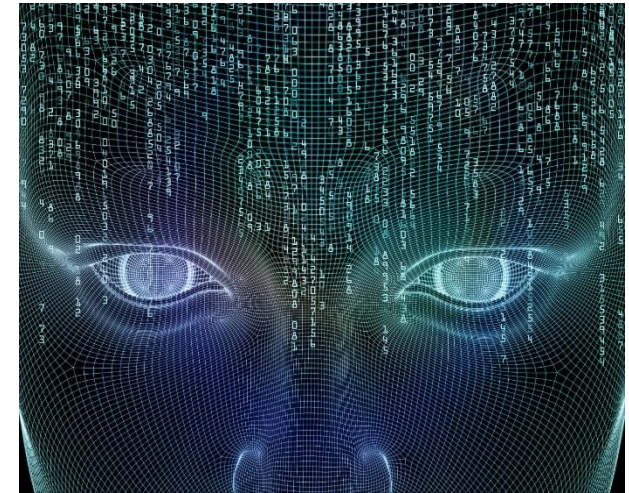
Claroty
Upstream
Escrypt
Blackberry
Cybellum
Blockharbor
C2A
Synopsis
Intsignts
ValiMail

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

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](#)