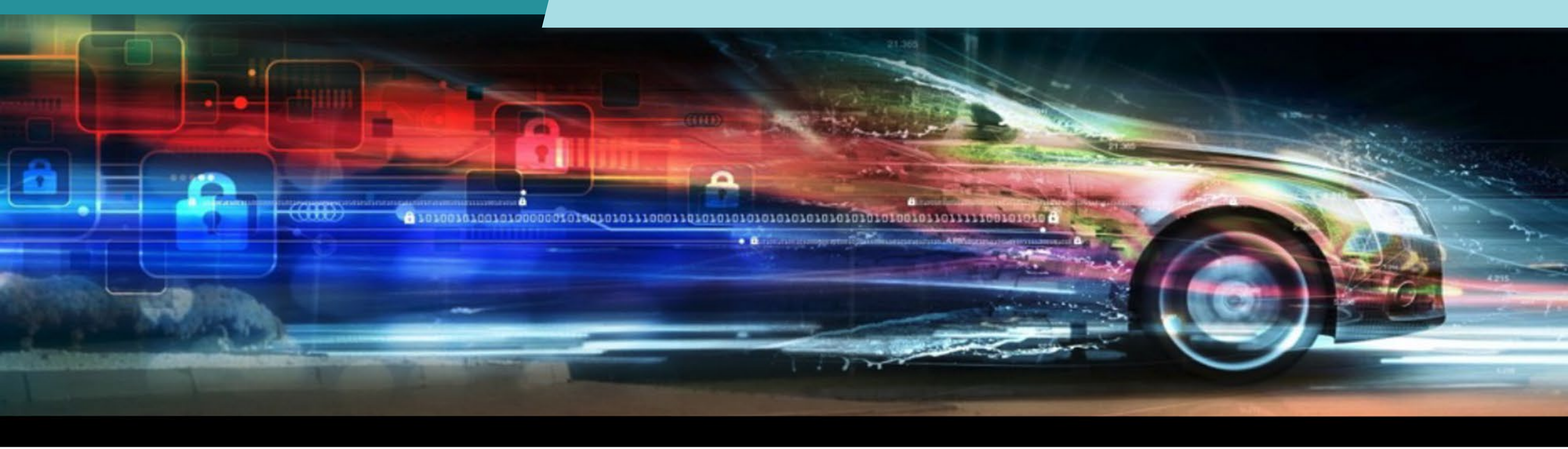


Welcome to Auto-ISAC!

Monthly Virtual Community Call

September 6, 2023

This Session will be recorded.

This document is Auto-ISAC Sensitive and Confidential.

TLP:CLEAR

AUTO-ISAC
Automotive Information Sharing and Analysis Center

Auto-ISAC Antitrust Statement

As Members of the Auto-ISAC, we strictly comply with EU and US antitrust laws. Please do not discuss anything that your company considers commercially sensitive and/or confidential such as pricing or future product plans. A violation of any of the above-mentioned issues will result in us having to quickly terminate the meeting.

Finally, please remember to keep these deliberations confidential. Please do not discuss the substance of these meetings outside of this group.

This meeting is being held at

TLP:CLEAR

Disclosure is not limited.

Traffic Light Protocol (TLP)

Version 2.0 Definitions

Color		When Should It Be Used?	How May It Be Shared?
TLP:RED 🔴⚫⚫	**Not for disclosure, restricted to participants only.**	Sources may use TLP:RED when information cannot be effectively acted upon without significant risk for the privacy, reputation, or operations of the organizations involved. For the eyes and ears of individual recipients only, no further.	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.
TLP:AMBER+STRICT ⚫🟡⚫	**Limited disclosure, restricted to participants' and its organization.**	Sources may use TLP:AMBER+STRICT when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organization.	Recipients may share TLP:AMBER+STRICT information only with members of their own organization on a need-to-know basis to protect their organization and prevent further harm.
TLP:AMBER ⚫🟡⚫	**Limited disclosure, restricted to participants' organization and its clients on a need-to-know basis.**	Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved. Note that TLP:AMBER+STRICT should be used to restrict sharing to the recipient organization only.	Recipients may share TLP:AMBER information with members of their own organization and its clients on a need-to-know basis to protect their organization and its clients and prevent further harm.
TLP:GREEN ⚫⚫🟢	**Limited disclosure, restricted to the community.**	Sources may use TLP:GREEN when information is useful to increase awareness within their wider community.	Recipients may share TLP:GREEN information with peers and partner organizations within their community, but not via publicly accessible channels. Unless otherwise specified, TLP:GREEN information may not be shared outside of the cybersecurity or cyber defense community.
TLP:CLEAR ⚪⚪⚪	**Disclosure is not limited.**	Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	Recipients may share this information without restriction. Information is subject to standard copyright rules.

Source: https://www.us-cert.gov/tlp

Agenda

Time (ET)	Topic
11:00	**Welcome** ➢ Why We're Here ➢ Expectations for This Community
11:05	**Auto-ISAC Update** ➢ Auto-ISAC Activities ➢ Heard Around the Community ➢ Intelligence Highlights
11:15	***DHS CISA Community Update*** ➢ **Jeff Terra, Consulting Support, Joint Cyber Defense Collaborative (JCDC), Cybersecurity and Infrastructure Security Agency (CISA)**
11:20	**Featured Speaker:** ➢ **Stephen Lilley, Partner, Mayer Brown LLP** ➢ **Title: *"Cyber Policy Developments Affecting the Auto Industry"***
11:45	**Around the Room** ➢ 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!"*

AUTO-ISAC
Automotive Information Sharing and Analysis Center

❖ Participate

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

30 *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

46 *Supplier & Commercial Vehicle Members*

20 *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)*

2023 Board of Directors

Thank you for your Leadership!

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

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

Stephen Roberts
***Secretary** of the*
Board of the Directors
Honda

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

Andreas Ebert
***Chair** of the EuSC*
Volkswagen

Andrew Hillery
***Chair** of the CAG*
Cummins

Ravi Puvvala
***Chair** of the SAG*
Fleet Defender

Monica Mitchell
Polaris

Bob Kaster
Bosch

Brian Witten
Aptiv

Auto-ISAC Member Roster

As of September 1, 2023

76 Members + 5 Pending

Aisin	Fleet Defender	Lucid Motors	Polaris
Allison Transmission	Flex	Luminar	Qualcomm
American Axle & Manufacturing	Ford	Magna	Renesas Electronics
Aptiv	Garrett	MARELLI	Rivian
AT&T	General Motors (Cruise-Affiliate)	Mazda	Stellantis
AVL List GmbH	Geotab	Mercedes-Benz	Subaru
Blackberry Limited	Harman	Mitsubishi Electric	Sumitomo Electric
BMW Group	Hitachi	Mitsubishi Motors	thyssenkrupp
BorgWarner	Honda	Mobis	Tokai Rika
Bosch (ETAS-Affiliate)	Hyundai	Motional	Toyota (Woven Planet-Affiliate)
Bose Automotive	Infineon	Navistar	Valeo
ChargePoint	Intel	Nexteer Automotive Corp	Veoneer
Continental (Argus-Affiliate)	John Deere Electronic	Nissan	Vitesco
Cummins (Meritor-Affiliate)	JTEKT	Nuro	Volkswagen (CARIAD-Affiliate)
Daimler Truck	Kia America, Inc.	Nuspire	Volvo Cars
Denso	Knorr Bremse	NXP	Volvo Group
e:fs TechHub GmbH	KTM	Oshkosh Corp	Waymo
Faurecia	Lear	PACCAR	Yamaha Motors
Ferrari	LG Electronics	Panasonic (Ficosa-Affiliate)	ZF

Pending: Amazon.com, CNH Industrial, Stoneridge , Phinia, Dana Inc.

Auto-ISAC Business Updates and Events

**All times are in ET

Upcoming Meetings:

- **Community Call:** Wednesday, October 4th Time: *11:00am – 12:00 p.m*. TLP:GREEN; Speaker: Brandon Barry, CEO, Block Harbor; Niraj Kaushik, MD North America, VicOne; Brian Gorenc, VP Threat Research Trend Micro, Title: *"Pwn2Own for Automotive @ Automotive World Tokyo"*

- **Partners Teaching Members:** Wednesday, September 20th Time: 10:00 am – 11:30 am TLP:AMBER; Speaker: Murtada Hamzawy, COO, Block Harbor "Knowledge Transfer & Retention in Automotive Cybersecurity, What Happens When an Automotive Cybersecurity Professional Leaves Your Organization & What to Do About It."

- **Auto-ISAC Summit** will be October 17th-18th, 2023 in Torrance, California. Complimentary pass codes were sent to Member POCs. Early bird registration discount pricing ends September 8th. Our discounted hotel room block ($219/night) closes September 21st. You can find more information here: https://automotiveisac.com/2023-annual-summit.
  - When booking travel, please consider joining these Members-only meetings in person:
    - Monday, Oct 16th, Q3 2023 Pre-Summit Joint PWG + IT/OT Workshop – In Person Only
    - Wednesday, Oct 18th, SBOM WG + JWG + Japan-Auto-ISAC Working Lunch meeting - HYBRID
    - Thursday, Oct 19th, Member Advisory Forum – HYBRID

Accelerating CASE Security

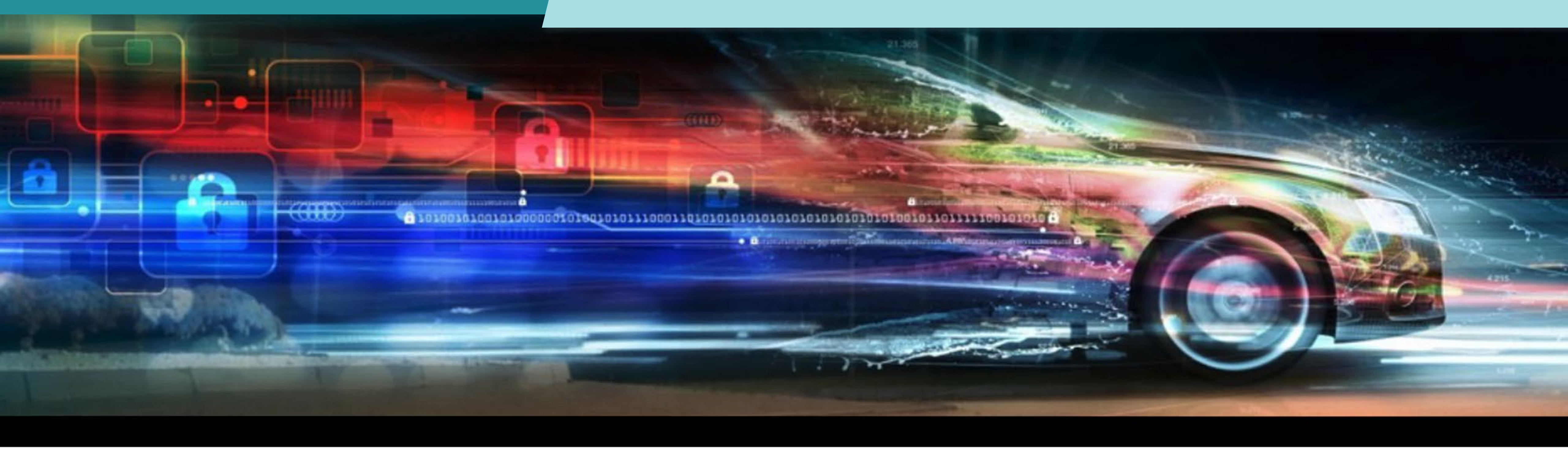
7th Annual Auto-ISAC Cybersecurity Summit

October 17-18, 2023

Torrance, CA

HONDA
The Power of Dreams

AUTO-ISAC



Auto-ISAC Intelligence Highlight

AUTO-ISAC INTELLIGENCE

- **Know what we track daily: subscribe to the DRIVEN; TLP:GREEN Auto-ISAC 2022 Threat Assessment released with Auto-ISAC Automotive Cyber Threat Ecosystem (1st Iteration) included.**
  - **Send feedback, contributions, or questions to analyst@automotiveisac.com**
- **Intelligence Notes**
  - **Geopolitical tensions involving Russia, China, North Korea, and Iran remain high with Russia-Ukraine in crisis (Russia-Ukraine, China, North Korea [1], Iran [2]).***
    - **Anonymous Sudan perpetrated a DDoS attack on Nigeria after the coup in Niger (NPR). There has since been another coup in Gabon (The Guardian).**
  - **Ransomware [3] Groups Targeting Automotive: Cl0p, LockBit 3.0, AlphV, Qilin, Lorenz**
  - **Malicious cyber tools and stolen data continue to be sold on forums including: XSS, BreachForums, DemonForums[dot]net, Dread, Kingdom Market.**
  - **Notable TTPs and Tools: Installing Web Shells on Citrix Servers (SecurityAffairs); Exploiting UEFI Implementation Flaws for Persistence (CISA); Exploiting Older Vulnerabilities (CISA); Deploying Ransomware via Managed Service Providers (DarkReading); Employing Cobra DocGuard in Supply Chain Attacks (Symantec); Leveraging Cisco VPNs to Infiltrate Networks (Rapid7, BleepingComputer); Employing Infected Removable Drives (Mandiant, Kaspersky); Employing Malicious Python Packages in Supply Chain Attacks (ReversingLabs); Dark AI Tools (Outpost24); Cloudzy (Halcyon); WoofLocker (Malwarebytes).**

CISA Resource Highlights

- Joint Cyber Defense Collaborative

Jeff Terra
9/6/2023

CISA Warns of Hurricane-Related Scams

CISA urges users to remain on alert for malicious cyber activity following natural disasters, such as hurricanes, as attackers target disaster victims and concerned citizens by leveraging social engineering tactics, techniques, and procedures (TTPs).

- Social engineering TTPs include
  - Phishing, in which threat actors pose as trustworthy persons/organizations—such as disaster-relief charities—to solicit personal information via email or malicious websites.

CISA recommends exercising caution in handling emails with disaster-related subject lines, attachments, or hyperlinks. In addition, be wary of social media pleas and texts messages related to severe weather events.

CISA Releases JCDC Remote Monitoring and Management (RMM) Cyber Defense Plan

The Remote Monitoring and Management (RMM) Cyber Defense Plan, is the first proactive Plan developed by industry and government partners through the Joint Cyber Defense Collaborative (JCDC).

- This plan addresses systemic risks facing the exploitation of RMM software.
  - Cyber threat actors can gain footholds via RMM software into managed service providers (MSPs) or manage security service providers (MSSPs) servers and, by extension, can cause cascading impacts for the small and medium-sized organizations.
- This release builds off the JCDC 2023 Planning Agenda and marks a major milestone in the continued evolution and maturation of the Collaborative's development to satisfy JCDC's core functions:
  - Developing and coordinating cyber defense plans
  - Operational collaboration and cybersecurity information fusion
  - Producing and disseminating cyber defense guidance

CISA, NSA, FBI, and International Partners Release Joint CSA on Top Routinely Exploited Vulnerabilities of 2022

- This advisory provides details on the top Common Vulnerabilities and Exposures (CVEs) routinely exploited by malicious cyber actors in 2022, and the associated Common Weakness Enumeration(s) (CWE), to help organizations better understand the impact exploitation could have on their systems.

- The authoring agencies urge all organizations to review and implement the recommended mitigations detailed in this advisory.

- The advisory provides vendors, designers, and developers recommendations on implementing **secure-by-design and -default principles and tactics** to reduce the prevalence of vulnerabilities in their software and end-user organizations' recommendations to reduce the risk of compromise by malicious cyber actors.

Security/Software Updates

For August 2023:

- Juniper Releases Multiple Security Updates
- Atlassian Releases Security Updates
- Fortinet Releases Security Updates
- Adobe Releases Security Updates
- Microsoft Releases Security Updates
- Mozilla Releases Security Updates
- CISCO Releases Security Updates
- VMWare Releases Security Updates

- **Best practices:**
  - Leverage automatic updates for all operating systems and third-party software
  - Implement security configurations for all hardware and software assets
  - Remove unsupported or unauthorized hardware and software from systems

Please note all information provided is TLP Amber

CISA Releases Industrial Control Advisories

- These advisories provide timely information about current security issues, vulnerabilities, and exploits surrounding ICS.
- For the period of 8/1/23- 8/31/23 approximately 36 advisories have been issued.
- Affected systems include Mitsubishi Electric, TELSTAR SCADA, Rockwell Automation, Schneider Electric, Sensormatic Electronics, Hitachi Energy, Siemens, CODESYS and many others.
- For current ICS advisories please check CISA.gov regularly

Please note all information provided is TLP Amber

KEVs Catalogue

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 added 8 new vulnerabilities to its Known Exploited Vulnerabilities (KEV) 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.

Please note all information provided is TLP Amber

Additional Resources from CISA

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

JOINT CYBER DEFENSE
COLLABORATIVE

For more information:

cisa.gov

Questions?

Central@cisa.dhs.gov

1-888-282-0870

Jeff Terra
9/6/2023

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*

30+ *Featured Speakers to date*

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!

7 *Best Practice Guides available on website*

2000+ *Community Participants*

Featured Speaker

Stephen Lilley

Partner, Mayer Brown

Stephen Lilley is a partner in the Washington DC office of Mayer Brown. He focuses his practice on helping clients navigate cutting-edge and interrelated litigation, regulatory, and policy challenges. A member of the firm's Cybersecurity & Data Privacy and Litigation practices, Stephen develops strategies to manage legal risks and to shape regulatory policy across a broad range of substantive areas. He has been named a "Leading Lawyer" for Cyber Law by the *Legal 500*.

Stephen has significant experience working with clients to identify, evaluate, and manage cybersecurity and data privacy risks; responding to cyber incidents and vulnerability disclosures; and defending businesses in related litigation. Stephen has particular experience advising on cybersecurity and national security issues relating to the Internet of Things, including vehicles and medical devices, and to manufacturing, critical infrastructure, and other industrial systems.

Stephen previously served as Chief Counsel to the Senate Judiciary Committee's Subcommittee on Crime and Terrorism, where he focused on cybersecurity issues.

MAYER | BROWN

Cyber Policy Update

PRESENTATION TO THE AUTO-ISAC

Stephen Lilley
Partner
slilley@mayerbrown.com
202-263-3865

SEPTEMBER 2023

US Policymakers Have Been Very Active on Cybersecurity—With More Developments on the Horizon

Five Key Themes

1. Earlier incident reporting or disclosure.
2. Intent to close perceived regulatory gaps.
3. Focus on software security.
4. Emphasis on governance.
5. Focus on all relevant technologies.

ONCD Continues to Implement the National Cyber Strategy

- The March 2023 cyber strategy called for a “[r]ebalanc[ing of] the responsibility to defend cyberspace,” and a “realign[ment of] incentives to favor long-term investments.”

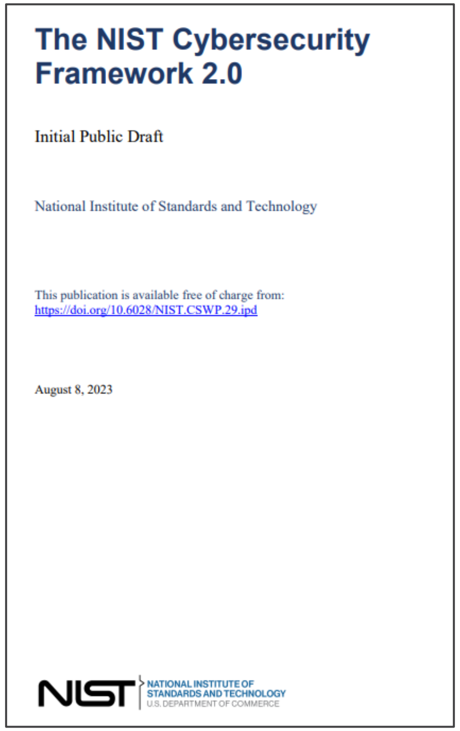
- ONCD released the implementation plan in July 2023 and the Administration is working through the various action items it contemplates, including:
  - Release of a request for information relating to regulatory harmonization;
  - Release of a request for information relating to the security of open source software;
  - Announcing an IoT labelling program, in coordination with the FCC.
- Further contemplated actions include:
  - Implementing FAR changes required under EO 14028;
  - Exploring approaches for shifting liability for software security.

Proposed Version 2.0 of the NIST Cybersecurity Framework Will Likely Further Increase the Impact of that Tool

- NIST released a draft of Version 2.0 of the NIST Cybersecurity Framework in August 2023.

- Key changes contemplated by the proposed draft include:
  - Removing "Critical Infrastructure" from its name to reflect broad and international use of framework;
  - Emphasizing governance by adding a sixth core function;
  - Including additional implementation guidance on the creation and use of "Framework Profiles" to help tailor cybersecurity priorities for specific sectors and use cases.

- The proposed draft is open for comment until November 4th.



The NIST Cybersecurity Framework 2.0

Initial Public Draft

National Institute of Standards and Technology

This publication is available free of charge from:
https://doi.org/10.6028/NIST.CSWP.29.ipd

August 8, 2023

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

CIRCIA Appears Likely To Have A Broad Impact Across Sectors

- CISA has responsibility for implementing the Cyber Incident Reporting for Critical Infrastructure Act.
- So far, CISA has requested comment through a request for information, but has not yet released a proposed rule.
- While it is difficult to predict, the Administration appears likely to implement CIRCIA broadly so that it covers a substantial number of companies—not just owners and operators of the *most* critical infrastructure.
- CISA is required to release a notice of proposed rulemaking by March 2024 and to release a final rule eighteen months later.

SEC Final Rules Require Public Company Cybersecurity Disclosures

- In July 2023, the SEC adopted new rules governing how public companies disclose their cyber risk management program and the material incidents they experience.

- The final rules would require registrants to:
  - Disclose material cybersecurity incidents within four business days of the company's determination that the cybersecurity incident is material
  - Make annual disclosures in form 10-K regarding the company's cybersecurity risk management and strategy
  - Make annual disclosures in Form 10-K regarding the company's cybersecurity governance, including with respect to oversight by the board and management

- The final rules build on staff guidance issued in 2011 and Commission guidance issued in 2018.

U.S. SECURITIES AND EXCHANGE COMMISSION ★ MCMXXXIV ★

Americas | Asia | Europe | Middle East

mayerbrown.com

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 and Partnership, please contact melissacromack@automotiveisac.com.

<u>Auto-ISAC Partnership Programs</u>

<u>Strategic Partnership</u>

- **For-profit** companies such as "Solutions Providers" that sell connected vehicle cybersecurity products & services.
- **Examples:** *Hacker ONE, Upstream, IOActive, Karamba, Grimm*

1. **Must be approved** by Executive Director and the Membership & Benefit Standing Committee (MBSC).
2. Formal agreements: **NDA, SPA, SoW, CoC** required.
3. **In-kind contributions** allowed. Currently <u>no fee</u>.
4. **Does not** <u>overtly sell or promote</u> 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.**

<u>Community Partnership</u>

- **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 (20)

ArmorText
BlockHarbor
Cybellum
Deloitte
FEV
GRIMM
HackerOne
Irdeto
Itemis
Karamba Security
KELA
Pen Testing Partners
Red Balloon Security
Regulus Cyber
Saferide
Security Scorecard
Trustonic
Upstream
VicOne
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 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
OASIS
ODNI
Ohio Turnpike & Infrastructure Commission
SANS
The University of Warwick
TSA
University of Tulsa
USSC
VOLPE
W3C/MIT
Walsh College

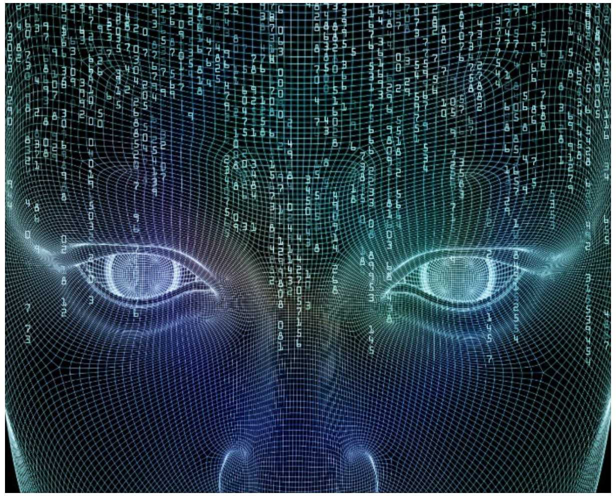
BENEFACTOR

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

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

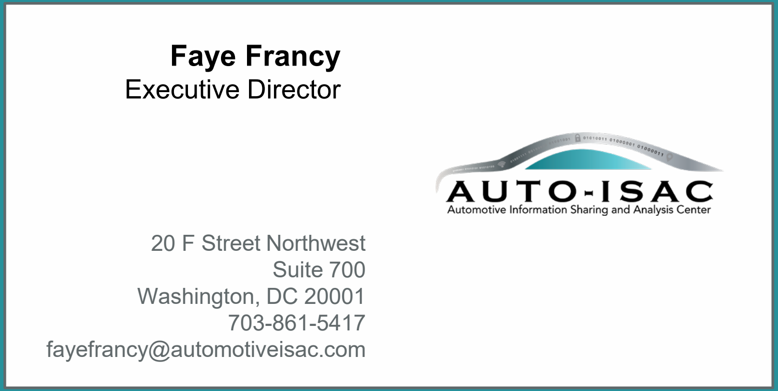


Building Resiliency Across the Auto Industry

Thank You

THANK
YOU
MAAKE
TERMA KASIH
RAIBH MAITH AGAT
JUSPAXAR
OBRIGADO
MATONDO
SALAMAT
KIITOS
MOCHCHAKKERAM
KIA ORA
MULTUMESC
CHOKRANE
SALAMAT
CAM ON BAN
GRAZIE
MULTUMESC
MERCI
MERCI
RAIBH MAITH AGAT
MERCI
MOCHCHAKKERAM
OBRIGADO
MOCHCHAKKERAM
GRAZIE
ASANTE
CHOKRANE
MATUR NUWUN
UA TSAUG RAU KOJ
MOCHCHAKKERAM
MATONDO
WELALIN
KIITOS
CHOKRANE
UA TSAUG RAU KOJ
DANK JE
RAIBH MAITH AGAT
SPASIBO
SPASIBO
MAAKE
OBRIGADO
ARIGATO
KIITOS
DANKON
MOCHCHAKKERAM
NIRRINGRAZZJAK
MOCHCHAKKERAM
OBRIGADO
SPASIBO
MULTUMESC
VINAKA
NIRRINGRAZZJAK
MAMANA
OBRIGADO
DANK JE

Our Contact Info



Faye Francy
Executive Director

AUTO-ISAC
Automotive Information Sharing and Analysis Center

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

AUTO-ISAC
Automotive Information Sharing and Analysis Center

AUTOMOTIVEISAC.COM