Welcome to Auto-ISAC!

Monthly Virtual Community Call

May 5, 2021

AUTO-ISAC
Automotive Information Sharing and Analysis Center

Happy Cinco De Mayo!

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 ➢ What's Trending
11:15	***DHS CISA Community Update***
11:20	**Featured Speaker:** ▪ **Norma Krayem**, *Vice President & chair, Cybersecurity, Privacy and Digital Innovation*, **Van Scoyoc Associates**
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!

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

40 *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

2021 Advisory Board (AB) Leadership

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

Member Roster

As of May 1, 2021

Highlighted = Change

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
Bosch (Escrypt-Affiliate)	LGE	Subaru
Continental	Luminar	Sumitomo Electric
Cummins	Magna	Tokai Rika
Denso	MARELLI	Toyota
Delphi Technologies	Mazda	TuSimple
FCA	Mercedes-Benz	Valeo
Ford	Meritor	Veoneer
Garrett	Mitsubishi Motors	Volkswagen
General Motors	Mitsubishi Electric	Volvo Cars
Geotab	Mobis	Volvo Group
Google	Motional	Waymo
Harman	Navistar	Yamaha Motors
Hitachi	Nexteer Automotive Corp	ZF
Honda	Nissan	*62 Members*

Business Administration

➢ Auto-ISAC Activities ***Members Only***

- **May 19, 2021** – ***Members Teaching Members, Aptiv*** –10:00 – 11:30 a.m. EDT. ***Presentation Topic*****:** TBA **TLP:AMBER. Members Only**

- ***CISO Executive Working Group*** established - Meeting ***Third Thursday of Every Month.***

➢ Community Activities:

➢ **June 2nd, 2021:** ***Community Call Speaker***: Tim Weisenberger , Project Manager, Technical Programs, Ground Vehicle Standards, **SAE International**

➢ ***Auto-ISAC Mid-year Community Call Survey***, will be sent after June Community Call. Please provide your thoughts and recommendations for improvement of this monthly engagement.

➢ **October 13-14, 2021:** ***Auto-ISAC Annual Cybersecurity Summit,*** 8:00 am – 5:00 pm

Intelligence and Analysis

Tristin Tharp

We would like to welcome a new addition to our Auto-ISAC Staff Team, Tristin Tharp. Tristin holds an MS from the University of Baltimore in Forensic Science- High Tech Crime and a BS in Political Science from Towson University.

Prior to her joining our organization, she has experience in DRP (Digital Risk Protection) at a local start-up company. She was the lead analyst on one of the largest financial service contracts at the company. In addition to her primary responsibilities, she built collaborative relationships with cross functional teams in order to meet organizational goals more effectively and efficiently. She also assisted the threat analyst team in the production of the annual threat prediction report this past year. Tristin brings her curious mind, persistent drive and diligent research skills to the Auto-ISAC.

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
Email us to request the Report, provide feedback, or ask questions

Intelligence Notes

- Malicious botnets are autonomously scanning the internet for vulnerable networks and deploying exploits (Sources: Recorded Future, Imperva, Security Affairs, Cybereason)
  - Consider vulnerabilities lurking in software supply chains of internet-connected cyber-physical systems and IT networks
  - Expect malicious botnet capabilities to continue to increase
- Ransomware operators are a dime a dozen. Focus ***less*** on (but do not ignore) ransomware group names, ***more*** on identifying and compiling infiltration tactics, techniques and procedures across ransomware groups
  - Vulnerability exploitation (Sources: Threatpost, Bleepingcomputer, Bleepingcomputer)
  - Social engineering/phishing and brute force attacks (Sources: Kaspersky, PCrisk)

CISA RESOURCE HIGHLIGHTS

TLP:WHITE–CISA Reduce the Risk of Ransomware Campaign

- **Launched in January 2021, concludes at the end of May 2021**
- **Includes weekly themes that are highlighted in toolkit resources at https://www[.]cisa[.]gov/publication/ransomware-campaign-toolkit**
- **CISA and MS-ISAC Joint Ransomware Guide that includes prevention best practices and response checklist at https://www[.]cisa[.]gov/publication/ransomware-guide**
- **One-stop Reduce the Risk of Ransomware resource at https://www[.]cisa[.]gov/ransomware**

TLP: WHITE – CISA Insider Threat Mitigation Resources

- **Includes resources to detect, assess and manage insider threats**
- **Highlights insider threat resources from the U.S. Secret Service, FBI and Carnegie Mellon**
- **Insider threat mitigation guide and other resources available at https://www[.]cisa[.]gov/publication/insider-threat-mitigation-resources**
- **Awareness and training resources highlighted during the September 2020 National Insider Threat Awareness Month at https://www[.]cdse[.]edu/toolkits/insider/awareness.html**
- **CISA Insider Threat web page at https://www[.]cisa[.]gov/insider-threat-mitigation**

TLP: WHITE – CISA Current Activity (CA) – Pulse Connect Secure Vulnerabilities

- **CISA released Alert AA21-110A: Exploitation of Pulse Connect Secure Vulnerabilities, as well as Emergency Directive (ED) 21-03, to offer technical details regarding this activity**
- **CISA highlighted Ivanti's release of their Pulse Secure Security Update on Monday May 3rd**
- **See:**
  - **https://us-cert[.]cisa[.]gov/ncas/current-activity/2021/05/03/ivanti-releases-pulse-secure-security-update**
  - **https://us-cert[.]cisa[.]gov/ncas/alerts/aa21-110a**
  - **https://cyber.dhs.gov/ed/21-03/**

TLP: WHITE – CISA CA - Exchange Server Vulnerability Response Updates

- **Update to AA21-062A to include MAR-10331466-1.v1 (China Chopper Webshell) and MAR-10330097-1.v1 (DearCry Ransomware)**
- **The CA highlights additional Exchange remediation resources from CISA**
- **https://us-cert[.]cisa[.]gov/ncas/current-activity/2021/04/12/updates-microsoft-exchange-server-vulnerabilities**

TLP:WHITE – CISA CA – SolarWinds-Related Resources

- **Use of the Aviary dashboard to help visualize and analyze outputs from Sparrow to detect possible compromised accounts and applications in Azure/Microsoft O365 environments**
- **https://us-cert[.]cisa[.]gov/ncas/current-activity/2021/04/08/using-aviary-to-analyze-post-compromise-threat-activity**
- **CISA and DoD Cyber National Mission Force (CNMF) analysis of SolarWinds-related malware referred to as SUNSHUTTLE and SOLARFLARE**
- **https://us-cert[.]cisa[.]gov/ncas/current-activity/2021/04/15/cisa-and-cnmf-analysis-solarwinds-related-malware**

TLP:WHITE – CISA CA – Malware Analysis Resources

- **Analysis Report – CISA Incident Response to SUPERNOVA Malware information available at:**
  - **https://us-cert[.]cisa[.]gov/ncas/current-activity/2021/04/22/cisa-incident-response-supernova-malware**
  - **https://us-cert[.]cisa[.]gov/ncas/analysis-reports/ar21-112a**
- **IOCs at:**
  - **https://us-cert[.]cisa[.]gov/sites/default/files/publications/AR21_112A.stix.xml**
  - **https://us-cert[.]cisa[.]gov/sites/default/files/publications/MAR-10319053-1.v1.WHITE_stix.xml**

TLP:WHITE – CISA CA – Codecov Releases New Detections for Supply Chain Compromise

- **Threat actor made unauthorized alterations of Codecov's Bash Uploader script, beginning on January 31, 2021**
- **Affected script remediated on April 1, 2021**
- **Following customer notification on April 15, update released on April 29**
- **Update includes new detections, including indicators of compromise and a non-exhaustive data set of likely compromised environment**
- **Complete CA, including vendor links available at https://us-cert[.]cisa[.]gov/ncas/current-activity/2021/04/30/codecov-releases-new-detections-supply-chain-compromise**

TLP: WHITE – Additional Resources From CISA

- CISA Homepage - https://www[.]cisa[.]gov/
- 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 Vulnerability Management (formerly known as the National Cyber Assessment and Technical Services (NCATS) program) - https://www[.]us-cert[.]gov/resources/ncats/
- CISA Cybersecurity Directives - https://cyber[.]dhs[.]gov/directives/
- CISA COVID-19 Response – https://www[.]cisa[.]gov/coronavirus

For more information:
cisa.gov

Questions?
CISAServiceDesk@cisa.dhs.gov
1-888-282-0870


CYBERSECURITY & INFRASTRUCTURE
CISA
SECURITY AGENCY

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

Slides available on our website – www.automotiveisac.com

Featured Speaker

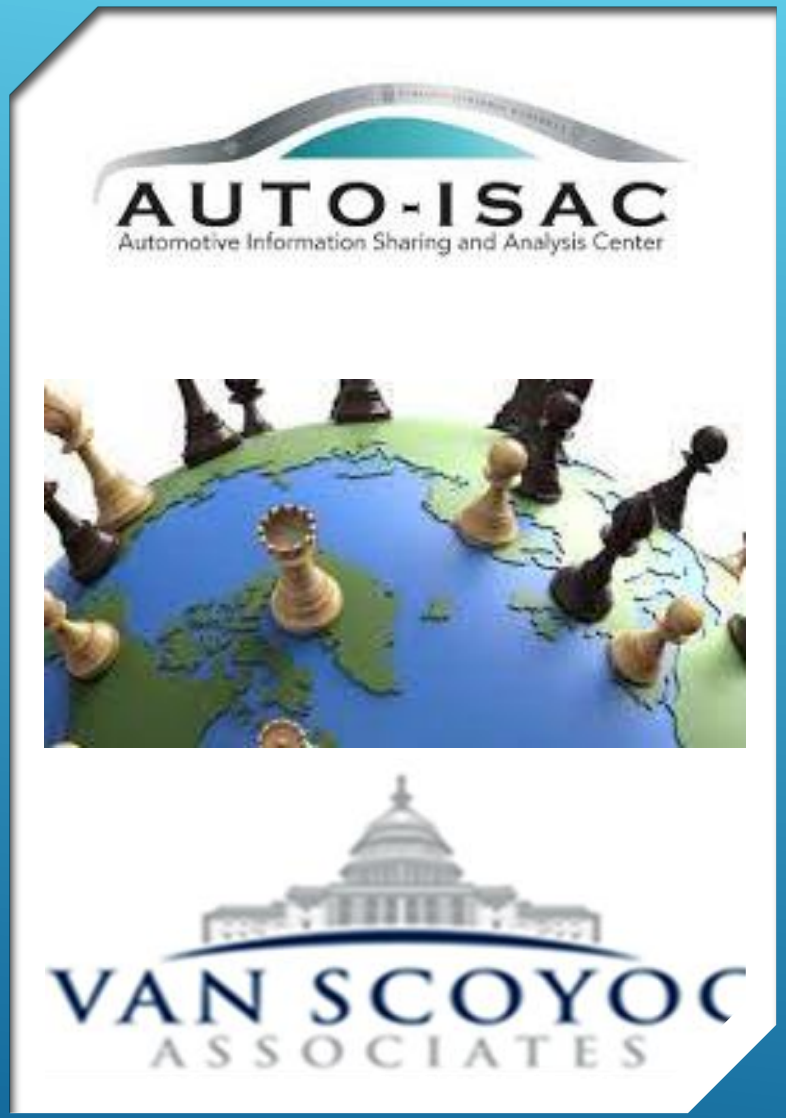
AUTO-ISAC
Automotive Information Sharing and Analysis Center

Norma Krayem- Van Scoyoc Associates

Vice President & chair, Cybersecurity, Privacy and Digital Innovation

Norma Krayem created one of the first-ever cybersecurity practices in 2005 in an AmLaw 100 law firm at a time when few understood what cybersecurity meant. She is an internationally recognized expert in cybersecurity and transportation matters, bringing more than 20 years of global experience having served at the U.S. Departments of State, Commerce, Transportation and FEMA as a consultant. She focuses on the intersection of trade, technology, defense, homeland security and cyber risk for clients in heavily regulated critical infrastructure sectors and brings a unique understanding of the nuances of traditional safety and physical security issues in the transportation sector coupled with her subject matter expertise on cybersecurity.

Ms. Krayem served as the Deputy Chief of Staff at the U.S. Department of Transportation (DOT) as well as the Chief of Staff and Deputy Administrator (Acting) of the Federal Railroad Administration. Prior to that, Ms. Krayem worked at the U.S. Department of State working on the G7 and held various senior positions at the U.S. Department of Commerce, within both the Office of the Secretary and the International Trade Administration. She is well versed in all of the policy, regulatory and compliance issues regulated and overseen by the U.S. Department of Transportation including autonomous vehicles, aviation, space, transit, rail, port/maritime, hazardous materials, pipelines, intelligent transportation systems, highway, motor carrier and more.



ON THE FRONT LINE: MANAGING 21ST CENTURY CYBERSECURITY RISKS MAY 5, 2021

Norma Krayem

Vice President and

Chair, Cybersecurity, Privacy & Digital Innovation Team

Van Scoyoc Associates

"The future battlespace is constructed of not only ships, tanks, missiles, and satellites, but also algorithms, networks, and sensor grids.

Like no other time in history, future wars will be fought on civilian and military infrastructures of satellite systems, electric power grids, communications networks, and transportation systems, and within human networks.

Both of these battlefields—electronic and human—are susceptible to manipulation by adversary algorithms.

Cortney Weinbaum and Lt Gen John N.T. "Jack" Shanahan, "Intelligence in a Data-Driven Age,"

Joint Force Quarterly 90, 2018

Agenda for Discussion

Cybersecurity is a National Security Imperative to the Biden-Harris Administration

White House

- New White House Executive Order addressing Russia
- New U.S. Treasury Department sanctions authority
- Multiple series of sanctions against all aspects of Russia, individuals and its economy
- U.S. formally names Russian Intelligence Services as the SolarWinds attacker

White House Executive Orders

1. 2021 White House Cybersecurity EO 13984: Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities
2. 2019 White House EO 13873: Securing the Information and Communications Technology and Services Supply Chain.
3. 2018 National Cybersecurity Strategy
4. 2017 White House EO 3800: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure
5. 2016 White House Presidential Policy Directive (PPD) 41

VAN SCOYOC ASSOCIATES

Cyber Risk is Much More Than Data Security: IIoT, IoT & Cyber-Physical Risks

IoT Connects Cyber & Physical Domains

Owners and Operators

vs.

Users

The Policy and Regulatory Landscape

Defining Critical Infrastructure Sectors

1. Health
2. Banking and Financial Services
3. Energy
4. Communications
5. Transportation
6. Chemical
7. Manufacturing
8. Food and Agriculture
9. Nuclear
10. Information Technology
11. Defense
12. Water and Wastewater
13. Dams
14. Government Facilities
15. Commercial Facilities
16. Emergency Services Sector

National Critical Functions (NCF)

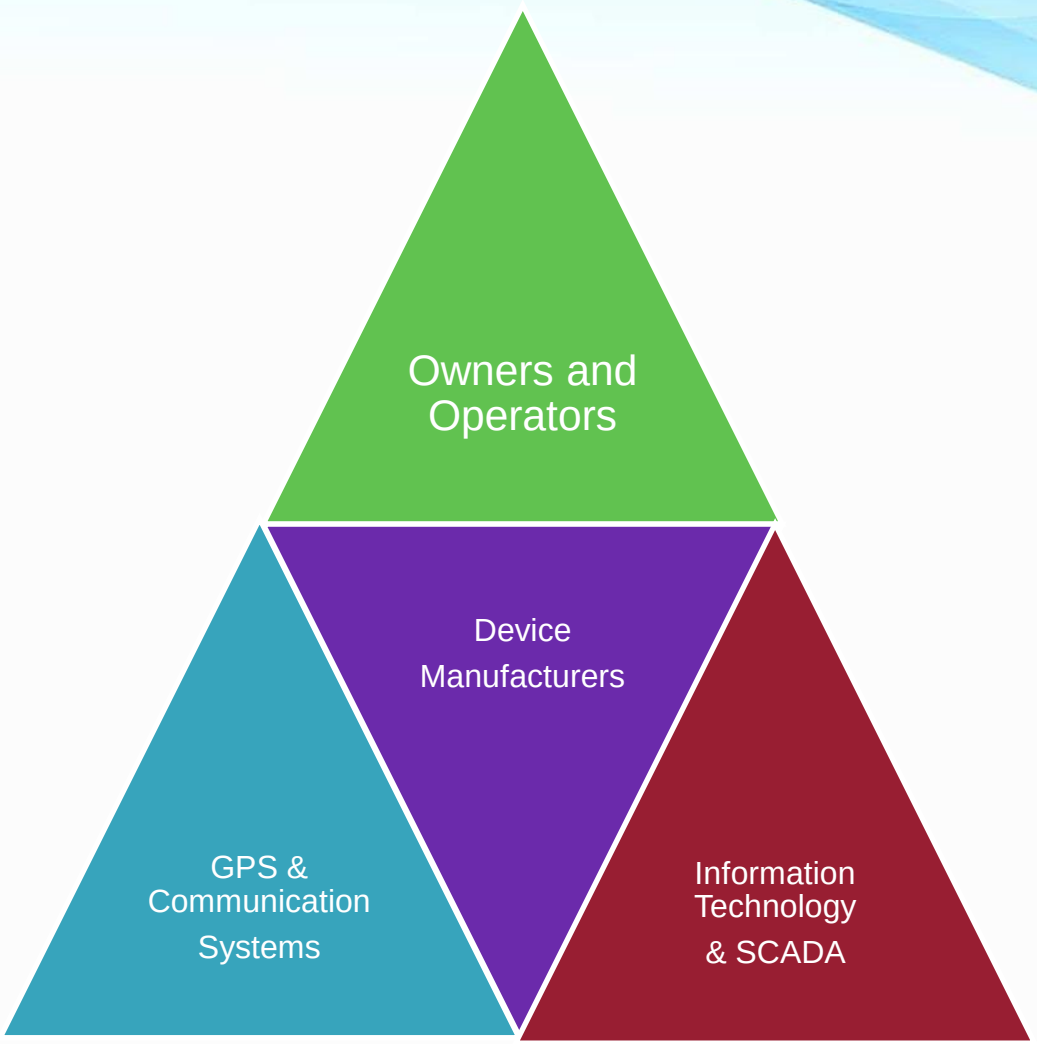
"The NCF construct provides a risk management lens that focuses less on a static, sector-specific or asset world view, and instead focuses on the functions an entity contributes to or enables. This allows for more holistically capturing cross-cutting risks and associated dependencies that may have cascading impact within and across sectors."

CONNECT	DISTRIBUTE	MANAGE	SUPPLY
▪ Operate Core Network ▪ Provide Cable Access Network Services ▪ Provide Internet Based Content, Information, and Communication Services ▪ Provide Internet Routing, Access, and Connection Services ▪ Provide Positioning, Navigation, and Timing Services ▪ Provide Radio Broadcast Access Network Services ▪ Provide Satellite Access Network Services ▪ Provide Wireless Access Network Services ▪ Provide Wireline Access Network Services	▪ Distribute Electricity ▪ Maintain Supply Chains ▪ Transmit Electricity ▪ Transport Cargo and Passengers by Air ▪ Transport Cargo and Passengers by Rail ▪ Transport Cargo and Passengers by Road ▪ Transport Cargo and Passengers by Vessel ▪ Transport Materials by Pipeline ▪ Transport Passengers by Mass Transit	▪ Conduct Elections ▪ Develop and Maintain Public Works and Services ▪ Educate and Train ▪ Enforce Law ▪ Maintain Access to Medical Records ▪ Manage Hazardous Materials ▪ Manage Wastewater ▪ Operate Government ▪ Perform Cyber Incident Management Capabilities ▪ Prepare for and Manage Emergencies ▪ Preserve Constitutional Rights ▪ Protect Sensitive Information ▪ Provide and Maintain Infrastructure ▪ Provide Capital Markets and Investment Activities ▪ Provide Consumer and Commercial Banking Services ▪ Provide Funding and Liquidity Services ▪ Provide Identity Management and Associated Trust Support Services ▪ Provide Insurance Services ▪ Provide Medical Care ▪ Provide Payment, Clearing, and Settlement Services ▪ Provide Public Safety ▪ Provide Wholesale Funding ▪ Store Fuel and Maintain Reserves ▪ Support Community Health	▪ Exploration and Extraction Of Fuels ▪ Fuel Refining and Processing Fuels ▪ Generate Electricity ▪ Manufacture Equipment ▪ Produce and Provide Agricultural Products and Services ▪ Produce and Provide Human and Animal Food Products and Services ▪ Produce Chemicals ▪ Provide Metals and Materials ▪ Provide Housing ▪ Provide Information Technology Products and Services ▪ Provide Materiel and Operational Support to Defense ▪ Research and Development ▪ Supply Water

National Critical Functions: The functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.

VAN SCOYOC ASSOCIATES

Cyber and Physical Risk - Internet of Things (IoT) and Industrial Internet of Things (IIoT)



Defining Cyber-Physical Systems

"Smart Infrastructures comprise several operators from different domains of activity, such as energy, public transport, public safety. They deploy and operate "cyber-physical systems," that are data-controlled equipment which interact with the physical world. They collaborate and exchange data under several schemes, depending on their level of maturity."

-ENISA

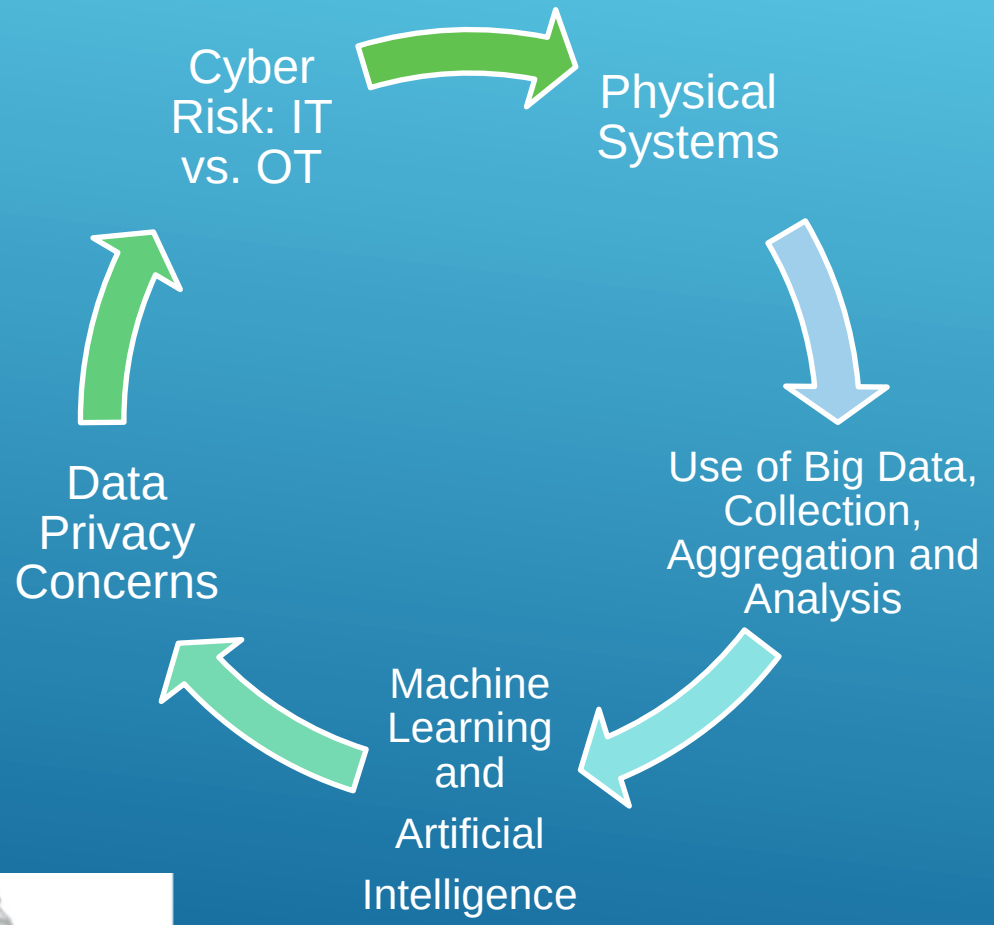
"Cyber-physical systems (CPS) are smart systems that include engineered interacting networks of physical and computational components. CPS and related systems (including the Internet of Things (IoT) and the Industrial Internet) are widely recognized as having great potential to enable innovative applications and impact multiple economic sectors in the worldwide economy."

-NIST SP 1500-201

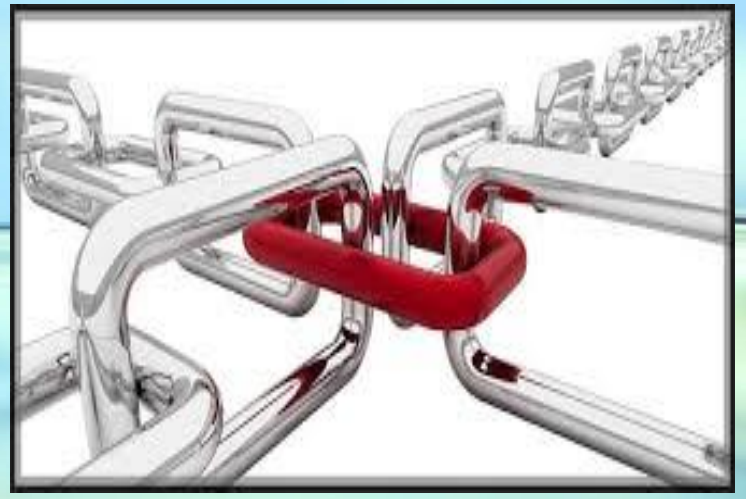
"These highly interconnected and integrated systems provide new functionalities to improve quality of life and enable technological advances in critical areas, such as personalized health care, emergency response, traffic flow management, smart manufacturing, defense and homeland security, and energy supply and use. In addition to CPS, there are many words and phrases (Industrial Internet, Internet of Things (IoT), machine-to-machine (M2M), smart cities, and others) that describe similar or related systems and concepts."

-NIST SP 1500-201

Technological Innovation and First to Market vs. Cyber, Privacy and Data Security Risks



VAN SCOYOC ASSOCIATES



Aggregated Risk Across All Sectors Based on Common Links

- DATA IN THE CLOUD
- SATELLITE, GPS, INDUSTRY
- IOT & MANUFACTURERS
- ARTIFICIAL INTELLIGENCE
- SMART CITIES
- IT AND TECHNOLOGY

Key Federal Strategies Impacting AV Issues

White House
National Security
Strategy

Cybersecurity
Executive Orders

THE WHITE HOUSE
WASHINGTON

U.S. DHS

CISA

TSA Cybersecurity
Roadmap

Transportation
Security
Administration

CISA

U.S. DOT

NHTSA

FMCSA

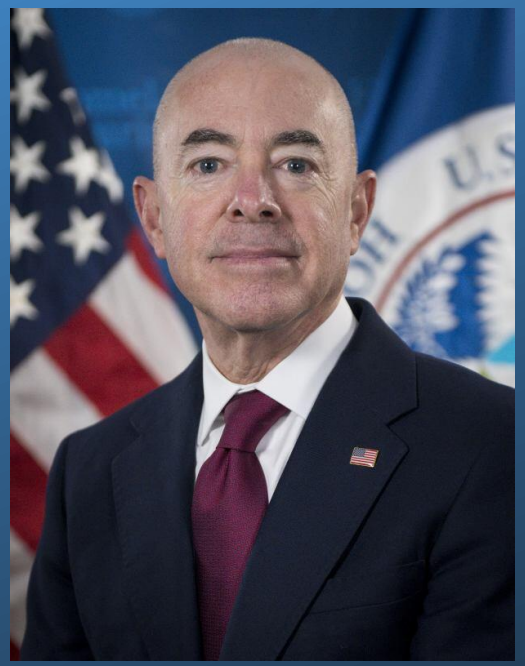
NHTSA
www.nhtsa.gov

FMCSA
Federal Motor Carrier Safety Administration

Transportation Security Administration

- In November 2018, TSA released a “Cybersecurity Roadmap” in which it outlined its role as the Agency in charge of the cybersecurity of the Transportation Systems Sector (TSS).
    - The TSA Cybersecurity Roadmap states that TSA will include cybersecurity in its risk and threat assessments of the TSS. As necessary, TSA will leverage existing oversight authority to conduct the assessments of stakeholder networks and contingency plans to ensure the resilience of the TSS. The Roadmap calls for TSA and our stakeholders to engage more on cybersecurity related issues. That information will include not just threat indicators and activity but also lessons learned, potential consequences, vulnerability-related details, and planning for response and recovery in the event of a cyber incident.
    - The United States Coast Guard is the SSA responsible for the Maritime Transportation Mode of the Transportation Systems Sector under the National Infrastructure Protection Plan (NIPP), which directs the Coast Guard to protect the Maritime Transportation System from cyber threats.
- In June 2020, TSA published an updated “Administrator’s Intent 2.0,” building on the ongoing response to the 2020 COVID-19 pandemic. It stresses:
    - TSA has expanded ability to analyze growing cyber, cargo, surface, and insider threats, and share transportation threat information to TSA security operations and transportation security partners and stakeholders for improved situation awareness, planning and threat mitigation
    - TSA will continue to advance cybersecurity initiatives to reduce cybersecurity risk and provide structured oversight to the Transportation Systems Sector

DHS to Prioritize Transportation Cybersecurity



On March 31, 2021, the Secretary of Homeland Security, Alejandro Mayorkas, laid out the cybersecurity priorities for DHS.

- **DHS Priorities**: The Secretary outlined three priorities for DHS in cyberspace. He stressed that DHS must: 1) work collaboratively with the private sector to protect U.S. critical infrastructure; 2) modernize Federal cyber defenses; and 3) unify Federal efforts in cyberspace.

- **CISA Implementation of Cyber Priorities**: During the event, Secretary Mayorkas announced a series of 60 day sprints to focus on urgent priorities, and a series of four other issues that CISA will continue to work on simultaneously.

- **60 Day Sprints:** This initiative will mobilize action by elevating existing efforts and creating dedicated actionable plans for urgent issues that need to be addressed. Sprints will include a focus on transportation systems, ICS systems, ransomware, international capacity building, and other issues over the next year.

Congress Picks Up Pace to Mandate Changes

Cyberspace Solarium Commission

- Created by Congress and named after Project Solarium created in 1953 by President Eisenhower to address the emerging Russia nuclear threat.
- 75 Legislative recommendations, 26 now law
- New efforts include: establishing liability for final goods assemblers of software, hardware, and firmware-- for damages from incidents that exploit known and unpatched vulnerabilities (4.2) for as long as they support a product or service and if known at the time of shipment or discovered and not fixed within a reasonable amount of time.

VAN SCOYOC ASSOCIATES

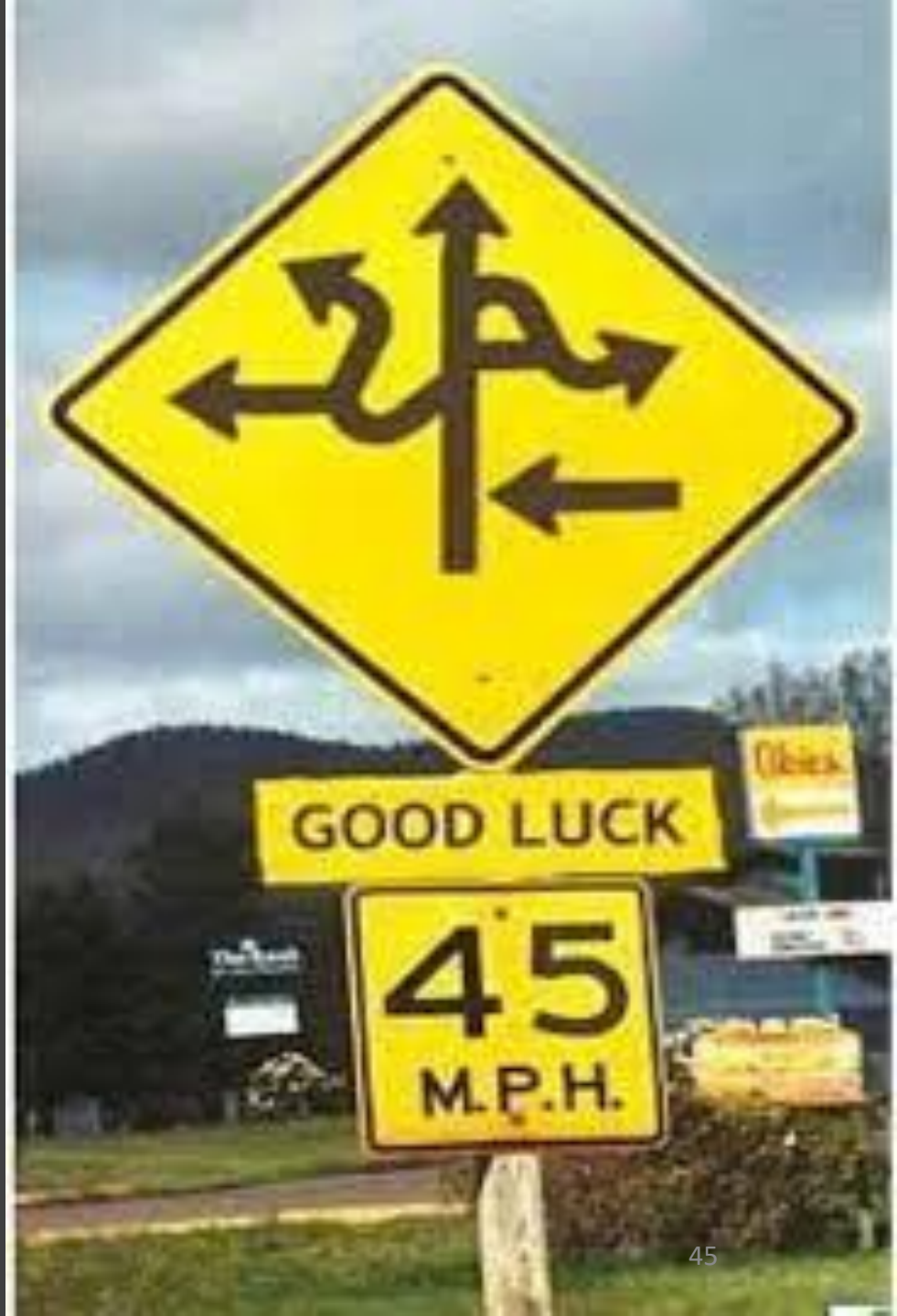
EU Review: Cybersecurity, AI and Autonomous Vehicle Risks

"When an insecure autonomous vehicle crosses the border of an EU Member State, so do its vulnerabilities. Security should not come as an afterthought, but should instead be a prerequisite for the trustworthy and reliable deployment of vehicles on Europe's roads," **said EU Agency for Cybersecurity Executive Director Juhan Lepassaar.**

February 11, 2021

The “regulator of record” for cybersecurity issues in the automotive sector and for autonomous vehicles while established in 2018, still needs clarification.

Transportation one of the few critical sectors not yet regulated for cybersecurity.



Top 14 Cyber and Data Privacy Issues to Look For in 2021

Norma Krayem
Vice President & Chair, Cybersecurity, Privacy and Digital Innovation
Van Scoyoc Associates
NKrayem@VSADC.com
+1-202-815-2331

VAN SCOYOC ASSOCIATES

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 or Partnership, please contact Auto-ISAC! fayefrancy@automotiveisac.com

Auto-ISAC Partnership Programs

Strategic Partner | **Community Partners**

Solutions Providers

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

Examples: Hacker ONE, IOActive, Karamba, Grimm

Associations

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

Examples: Auto Alliance, ATA, ACEA, JAMA

Affiliations

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

Examples: NCI, DHS, NHTSA, Colorado State

Community

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

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

INNOVATOR
Paid Partnership

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

NAVIGATOR
Support Partnership

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

COLLABORATOR
Coordination Partnership

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

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)

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

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!


thank you
рахмат
danke
謝謝
ngiyabonga
شكراً جزيلاً
spas
teşekkür ederim
Баярлалаа
mersi
kia ora
barka
welalin
tack
mahalo
спасибо
faafetai lava
vinaka
blagodaram
dank je
misaotra
matondo
paldies
grazzi
tapadh leat
спасибі
kiitos
dankie
gracias
хвала
nanni
nandri
dhanyavad
asante
manana
mauruuru
köszönöm
aciu
obrigada
tenki
bedankt
bayarlalaa
gràcie
hvala
dankon
djiere dieuf
tau
mochchakkeram
murakoze
enkosi
akun
дякую
mamnun
dziękuję
chnorakaloutioun
gratias ago
gràcies
sulpáy
go raibh maith agat
chokrane
sobodi
děkuji
sukriya
kop khun krap
taiku
obrigado
sagolun
arigatô
takk
dakujem
trugarez
mèsi
ありがとう
tanemirt
grazie
didi madloba
najis tuke
terima kasih
rahmet
diolch
dhanyavadagalu
shukriya
mercê
мерси
kam sah hamnida
rahmat
xièxie
ευχαριστώ
merci
감사합니다
তোমাকে ধন্যবাদ

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

20 F Street NW, Suite 700
Washington, DC 20001
sharmilakhadka@automotiveisac.com

AUTO-ISAC
Automotive Information Sharing and Analysis Center

www.automotiveisac.com
@auto-ISAC