



# **WELCOME TO AUTO-ISAC!**





## ***MONTHLY VIRTUAL COMMUNITY CALL***

October 6, 2021

TLP:WHITE



# DHS TRAFFIC LIGHT PROTOCOL (TLP) CHART

COLOR	WHEN SHOULD IT BE USED?	HOW MAY IT BE SHARED?
<p><b>TLP:RED</b></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><b>TLP:AMBER</b></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><b>TLP:GREEN</b></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><b>TLP:WHITE</b></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	<b>Welcome</b> <ul style="list-style-type: none"><li>➤ Why We're Here</li><li>➤ Expectations for This Community</li></ul>
11:05	<b>Auto-ISAC Update</b> <ul style="list-style-type: none"><li>➤ Auto-ISAC Activities</li><li>➤ Heard Around the Community</li><li>➤ What's Trending</li></ul>
11:15	<b><i>DHS CISA Community Update</i></b>
11:20	<b>Featured Speaker:</b> <ul style="list-style-type: none"><li>▪ <b>Mr. Darrell Russell</b> <i>Director of Operations-Vehicles, National Insurance Crime Bureau (NCIB)</i></li></ul>
11:45	<b>Around the Room</b> <ul style="list-style-type: none"><li>➤ Sharing Around the Virtual Room</li></ul>
11:55	<b>Closing Remarks</b>

# 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](mailto: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 (1<sup>st</sup> 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)*



# 2020 - 2021 BOARD OF DIRECTORS

## EXECUTIVE COMMITTEE (EXCOM)

**2022-2023**  
**Elections coming!**



**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**

## 2020 - 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 OCTOBER 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

- **Wednesday, October 27 – 4Q21 Europe Workshop** from 7 – 11:00 a.m. ET (1 - 5:00 p.m. CET). Agenda to come. **Registration is open.**

## ➤ Community Call: TLP: GREEN

- **Date/Time:** Wednesday, November 3, 11 – 12:00 p.m.
- **Speaker:** Kate McClaskey, DHS Program Lead, CISA DHS
- **Title:** *Autonomous Ground Vehicle Security: Transportation Systems Sector*

## ➤ 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**
- **LAST Call - Please REGISTER!!!**





**AUTO-ISAC CYBERSECURITY SUMMIT | OCT 13-14<sup>TH</sup> | 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](mailto: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
  - Despite the US Treasury Department's sanctions on Suex, a cryptocurrency exchange operating in Russia, and the US Government's initiative bringing together 30-nations to combat ransomware, **DO NOT** let your guard down; ransomware attacks will continue to pose a daily threat to your organization. **DO** have incident response and recovery plans. ([SecurityWeek](#), [Politico](#), [Department of the Treasury](#), [BleepingComputer](#))
  - Malware targeting mobile devices appears to be increasing in complexity. Closely monitor new reporting of vulnerabilities and malware targeting mobile devices and apps. Assess related risks to your products and critical systems ([ZDNet](#), [CloudMark](#), [ThreatPost](#), [The Hacker News](#)).

# CISA RESOURCE HIGHLIGHTS



# TLP: WHITE – CISA Cybersecurity Awareness Month 2021

- **Four (4) Weekly Themes:**
  - **Be Cyber Smart.**
  - **Phight the Phish!**
  - **Explore. Experience. Share. – Cybersecurity Career Awareness Week**
  - **Cybersecurity First**
- **Resources:**
  - [https://www\[.\]cisa\[.\]gov/cybersecurity-awareness-month](https://www[.]cisa[.]gov/cybersecurity-awareness-month)
  - [https://staysafeonline\[.\]org/cybersecurity-awareness-month/](https://staysafeonline[.]org/cybersecurity-awareness-month/)



# TLP: WHITE – CISA Fourth Annual National Cybersecurity Summit

- Four (4) themes that focus on CISA’s mission to “Defend Today, Secure Tomorrow“:
  - Oct. 6: Assembly Required: The Pieces of the Vulnerability Management Ecosystem
  - Oct. 13: Collaborating for the Collective Defense
  - Oct. 20: Team Awesome: The Cyber Workforce
  - Oct. 27: The Cyber/Physical Convergence
- Register at [https://www\[.\]Eventbrite\[.\]com/e/169672754777](https://www[.]Eventbrite[.]com/e/169672754777)
- More information at:
  - [https://www\[.\]cisa\[.\]gov/cybersummit2021](https://www[.]cisa[.]gov/cybersummit2021)
  - [https://www\[.\]cisa\[.\]gov/news/2021/09/08/cisa-host-fourth-annual-national-cybersecurity-summit](https://www[.]cisa[.]gov/news/2021/09/08/cisa-host-fourth-annual-national-cybersecurity-summit)



# TLP: WHITE – CISA Current Activity Highlights

- **CISA Insights on Risk Considerations for Managed Service Provider Customers**
  - [https://us-cert\[.\]cisa\[.\]gov/ncas/current-activity/2021/09/03/cisa-insights-risk-considerations-managed-service-provider](https://us-cert[.]cisa[.]gov/ncas/current-activity/2021/09/03/cisa-insights-risk-considerations-managed-service-provider)
- **CERT NZ Releases Ransomware Protection Guide for Businesses**
  - [https://us-cert\[.\]cisa\[.\]gov/ncas/current-activity/2021/09/14/cert-nz-releases-ransomware-protection-guide-businesses](https://us-cert[.]cisa[.]gov/ncas/current-activity/2021/09/14/cert-nz-releases-ransomware-protection-guide-businesses)
- **ACSC Releases Annual Cyber Threat Report**
  - [https://us-cert\[.\]cisa\[.\]gov/ncas/current-activity/2021/09/16/acsc-releases-annual-cyber-threat-report](https://us-cert[.]cisa[.]gov/ncas/current-activity/2021/09/16/acsc-releases-annual-cyber-threat-report)



# TLP: WHITE – Joint Cybersecurity Advisories

- **CISA, FBI, and NSA Release Joint Cybersecurity Advisory on Conti Ransomware**
  - [https://us-cert\[.\]cisa\[.\]gov/ncas/current-activity/2021/09/22/cisa-fbi-and-nsa-release-joint-cybersecurity-advisory-conti](https://us-cert[.]cisa[.]gov/ncas/current-activity/2021/09/22/cisa-fbi-and-nsa-release-joint-cybersecurity-advisory-conti)
  - [https://us-cert\[.\]cisa\[.\]gov/ncas/alerts/aa21-265a](https://us-cert[.]cisa[.]gov/ncas/alerts/aa21-265a)
- **FBI-CISA-CGCYBER Advisory on APT Exploitation of ManageEngine ADSelfService Plus Vulnerability**
  - [https://us-cert\[.\]cisa\[.\]gov/ncas/current-activity/2021/09/16/fbi-cisa-cgcyber-advisory-apt-exploitation-manageengine](https://us-cert[.]cisa[.]gov/ncas/current-activity/2021/09/16/fbi-cisa-cgcyber-advisory-apt-exploitation-manageengine)
  - [https://us-cert\[.\]cisa\[.\]gov/ncas/alerts/aa21-259a](https://us-cert[.]cisa[.]gov/ncas/alerts/aa21-259a)





# TLP: WHITE – Additional Resources From CISA

- CISA Homepage - [https://www\[.\]cisa\[.\]gov/](https://www[.]cisa[.]gov/)
- CISA NCAS – <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 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](mailto: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



# DARRELL RUSSELL, NICB

## *DIRECTOR OF OPERATIONS-VEHICLES*



**D.T. “Rusty” Russell** is the Director of Operations-Vehicles with the National Insurance Crime Bureau (NICB). In his role he coordinates all vehicle, marine, and specialized equipment investigative programs both nationally and internationally.

He has been with NICB since 2009 and previously served as an NICB Special Agent in Western North Carolina.

Prior to joining NICB, Rusty Russell retired from the Saint Lucie County Sheriff’s Office, spending the last fourteen years of his law enforcement career as a detective assigned to the auto theft division.

# NICB Overview

**Rusty Russell**

Director of Operations-Vehicles



# About NICB

- For **more than a century**, NICB's Intelligence Analysts and Investigators have aided the industry and law enforcement in combatting insurance crime
- We assist nearly **1,200 member companies** in **predicting, preventing, and prosecuting insurance crimes**
- We have a **robust network of strategic relationships** with insurers, law enforcement agencies, data providers, and other anti-fraud organizations







## **Our Mission**

Through intelligence-driven operations, NICB leads a united effort to combat and prevent insurance crime.

## **Our Vision**

To be the preeminent organization fighting insurance crime.

# Our Core Pillars



*Intelligence,  
Analytics, and  
Operations*



*Education and  
Crime Prevention*



*Strategy,  
Policy, and  
Advocacy*

# Intelligence, Analytics, & Operations

- Uniquely positioned to **investigate multi-claim, multi-carrier insurance fraud**
- **Innovative approaches** to identify and **leverage unique intelligence sources**
- **Established partnerships** with local, state, and federal law enforcement agencies along with data providers and anti-fraud organizations
- **World renowned vehicle identification expertise**



# Education & Crime Prevention

- NICB serves as the **authority on insurance crime trends and prevention measures** to inform and engage the public
- **Standardized training curriculum** for **entry-level to advanced** analysts and investigators
- National Insurance Crime Training Academy (NICTA) provides the **largest and most robust fraud curriculum**
  - On-demand courses and weekly webinars facilitated by experienced agents and industry experts



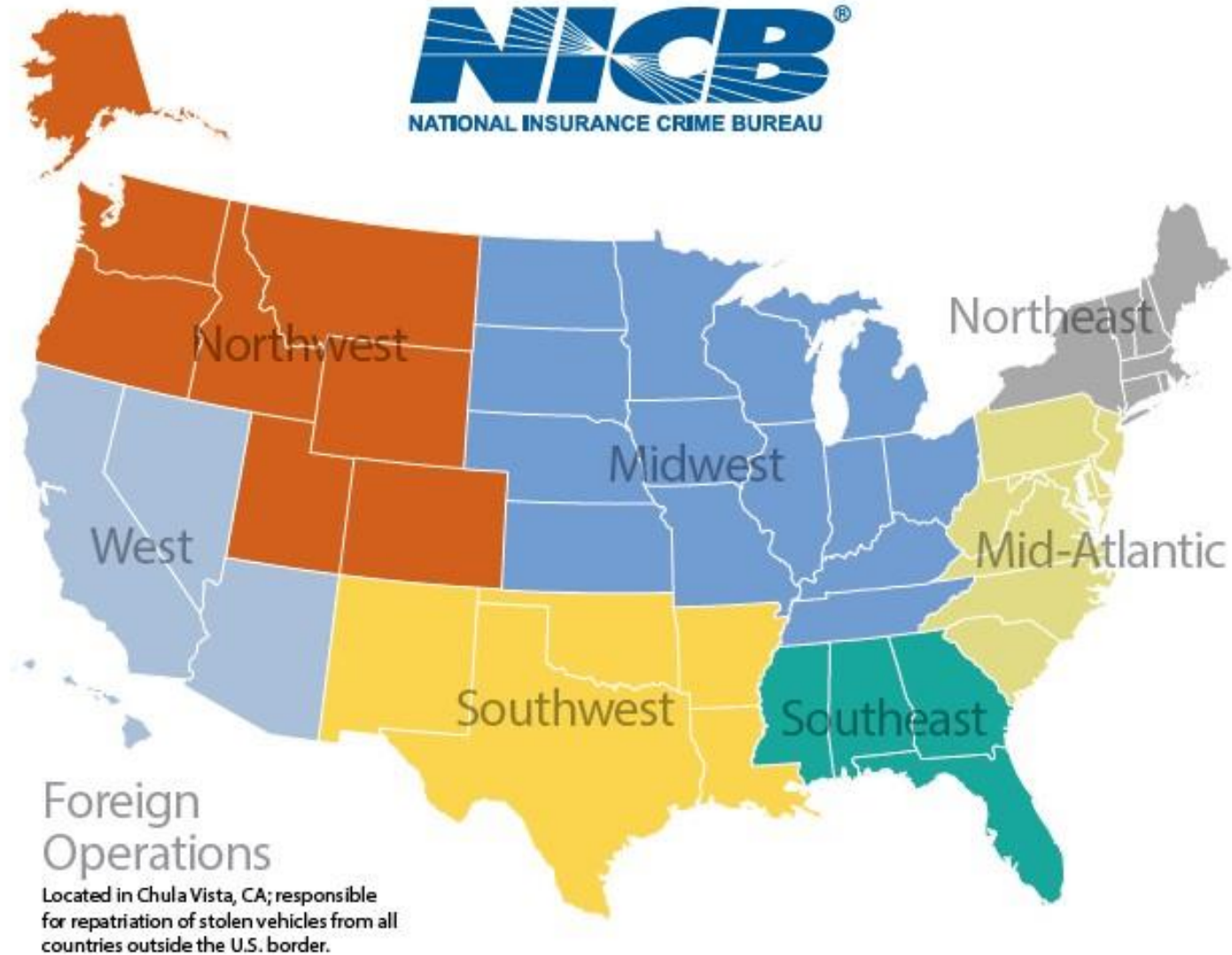
# Evolving Our Data Capability

- As insurance crime threats increase in frequency and complexity, **NICB is leveraging data analytics to identify unknown criminal networks and better forecast crime trends**
- **NICB is uniquely positioned in the industry** to lead the fraud data analytics efforts
- Working collaboratively with stakeholders, **NICB will utilize data analytics responsibly** to prevent and combat insurance crimes, consistent with law and regulations



# Where We Are

- Approximately 190 NICB Special Agents are strategically located throughout the U.S.
  - Law enforcement and insurance industry experience
  - Law enforcement contacts and liaison
  - State and Federal agencies' contacts and liaison



# How We Investigate

- Collect and analyze questionable medical, commercial, vehicle, and property fraud claims
- Provide ForeWARN<sup>SM</sup> and MedAWARE<sup>SM</sup> alerts to NICB members
- Conduct joint investigations
- Support prosecutive efforts



# Multi-Claim Investigations

NICB works to identify and shut down multi-claim fraud rings and provides law enforcement with evidence to help prosecute the criminals involved.

- Casualty Fraud
  - Attorney Activities
  - Illegal Solicitations
  - Runners, Chasers and Cappers
  - Kickback and Bribery





# NICB Managed Data

- NICB Information Sources
  - Shipping and Assembly
  - NCIC/CPIC Mirror Image
  - License Plate Reader File
  - Vehicle Impounds
  - Manufacturer Key Code Transaction Data

# NICB Managed Data

- NICB Information Sources (cont.)
  - Geospatial Intelligence
  - NICB Intelligence Database
  - Rental Fleet Inventory
  - Boat/Vessel File
  - NICB Case and *ForeWARN*<sup>SM</sup> Alert Indicator



# IA Group

- Customer Contact / Call Center
- 13 people divided into two teams
- Hours of operation: 7- 7 pm Mon – Fri
- Phone: 800-447-6282 x 7002
- Email: [IA@NICB.org](mailto:IA@NICB.org)

# What Does an IA Do and for Who?

Conducts research and disseminates information that aids in the identification and recovery of stolen vehicles and suspect insurance claims.

Assists by Phone/Email to:

- Member Companies
- Law Enforcement Agencies
- NICB Agents
- General Public (VINCheck Validation)
- Manufacturers
- Vendors

# Law Enforcement Support

- Vehicle identification
  - Provide secondary VIN locations
  - Cross-reference component parts
  - Surveillance videos
- Suspect runs
- Claim information

# Suspect Runs

- Suspect Runs / Data Runs
- Conducted by utilizing all or a combination of the following
  - Vehicle description
  - Model year
  - Geographical area
  - ORI
  - Date Range
  - Damage description

# Surveillance Videos/Photos

Identify Possible Year,  
Make, Model

- Abductions
- Shootings
- Robberies
- Hits and Runs



# Color Codes

- Provide color codes for list of VINs
- Provide list of certain color of vehicle





# Electronic Data in Vehicles

- NICB is currently using Berla iVE to access infotainment data in vehicles.
- Agents have been specially trained and certified to use this system.
- iVE currently support the acquisition and analysis of over 15,000 vehicles.
- Not all vehicles are compatible.



# Assistance with Infotainment Data

The combination of information and entertainment

Connects the occupants to their digital world

Provides information on vehicle performance, scheduled maintenance, and current status

Generally interacts directly with occupants and is main focal point



# What Information is Available?

- Connected Devices
  - Bluetooth, USB or wireless
  - Unique identifiers of the paired phones
  - Subscriber numbers
  - Contact lists
  - Call logs
  - SMS (text) messages
  - Media files



# What Information is Available?

- Location Data
  - Track logs
  - Saved locations
  - Routes
  - Internal system or mobile device-if connected



# What Information is Available?

- Vehicle Events
  - Door open/close
  - Gear shift
  - Odometer readings
  - Vehicle ignition
  - Speed logs



# Electronic Data in Vehicles

- NICB is currently using Bosch's CDR Tool to access Event Data.
- Not a black box in an airplane
- Found on 1996 & newer vehicles
- Requires an "event" to trigger recording



# What's an Event?

- Event = Crash or other physical occurrence that causes the trigger threshold to be met or exceeded, or any non-reversible deployment restraint to be deployed, whichever occurs first.
- Also known as change in Delta V.
- > 5 mph change in velocity



# Crash Data Retrieval (CDR) Tool

- Built by Bosch
- The device in the vehicle is the EDR, the tool used to retrieve the information is the CDR
- CDR does not change, erase, remove or alter any data. It cannot “reset” data or the module containing the data
- EDR data may be overwritten by other newer events or circumstances





# What's Required?

- NICB requires a Search Warrant or other official court document
- While the law enforcement agency may feel “consent” is sufficient this will not meet our internal requirements



# Differences between Berla & EDR

## ■ Infotainment System

- Not Event Driven
- Constantly recording data
- data stored days/weeks/months
- Interacts with external devices
- Extends to personal data
- Usually requires disassembly of center stack, very invasive
- Conducted pursuant to Court Order (search warrant)

## ■ Event Data Recorder

- Event Driven
- Requires trigger event to record
- 5 sec before/duration of event
- No interaction with devices
- No personal data
- May require removal of ACM-dependending on extent of damage
- Conducted pursuant to Court Order (search warrant)



**Thank You!**  
**Any 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](mailto:andreaschunn@automotiveisac.com).  
For Partnership, please contact [sharmilakhadka@automotiveisac.com](mailto: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-**

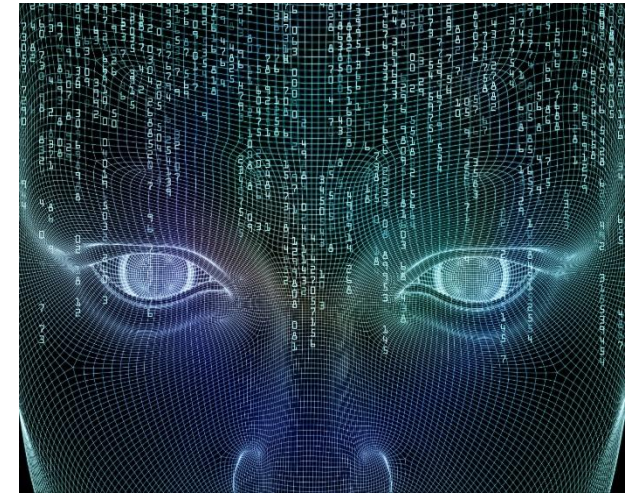
Claroty  
Upstream  
Escrypt  
Blackberry  
Cybellum  
Blockharbor  
C2A  
Synopsis  
Intsignts  
ValiMail

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