



AUTO-ISAC

MONTHLY COMMUNITY CALL

April 1, 2020



COVID-19

OUR THOUGHTS AND PRAYERS GO OUT TO ALL THOSE AFFECTED BY COVID-19. WE ARE VERY GRATEFUL TO OUR MEMBERS AND PARTNERS FOR THEIR CONTINUED SUPPORT AND ENGAGEMENT DURING THESE UNPRECEDENTED TIMES. IF WE CAN ASSIST IN ANY MANNER, PLEASE LET US KNOW HOW WE MIGHT HELP.



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 overview ➤ Heard around the community ➤ What's Trending
11:15	<i>DHS CISA Community Update</i>
11:20	Featured Speakers – <i>OmniAir Consortium – Jason Conley</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

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 Auto-ISAC Staff (staff@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!”*

19

*Navigator
Partners*

❖ Participate

- ❖ Participate in monthly virtual conference calls (1st Wednesday of month)
- ❖ If you have a topic of interest, connect with Auto-ISAC Staff–
staff@automotiveisac.com
- ❖ Engage & ask questions!

12

*Innovator
Partners*

20

OEM Members

❖ 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

38 *Supplier &
Commercial
Vehicle Members*

*Membership represents 99%
of cars on the road in North
America*

*Coordination with 23
critical infrastructure ISACs
through the National ISAC
Council*

AUTO ISAC – 2020 WAY FORWARD

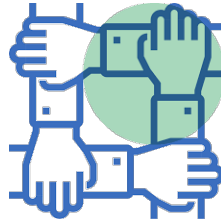
RE-EVALUATION OF STRATEGY & MISSION

*Who We Are &
Why We Are Here*

MISSION: *To strengthen the global automotive industry against cyber threats and enhance cyber attack resilience and response. **An attack on one is an attack on all.***



Timely Sharing of
Threat & Vulnerability
Information



Building
Strong
Relationships



Developing
Effective
Response Plans



Ensuring & Maturing
Consistent Cyber
Capability

Each Member is expected to: Trust, Share, Teach, Learn, Act

We are a **technical organization**, serving membership by enabling **cyber learning and capability development**. As members, we are expected to both **share and learn**, and continue to strengthen capabilities to protect our customers.
We will hold ourselves accountable.

Auto ISAC – 2020 Way Forward

ROLES, RESPONSIBILITIES
& METRICS

*Measuring
Success*

VALUE STREAMS & PERFORMANCE INDICATORS

Top Line Goal: Zero safety related cyber events in the industry



INFO SHARING & AWARENESS

% Participation
Sharing / Platform /
Attendance

EDUCATION

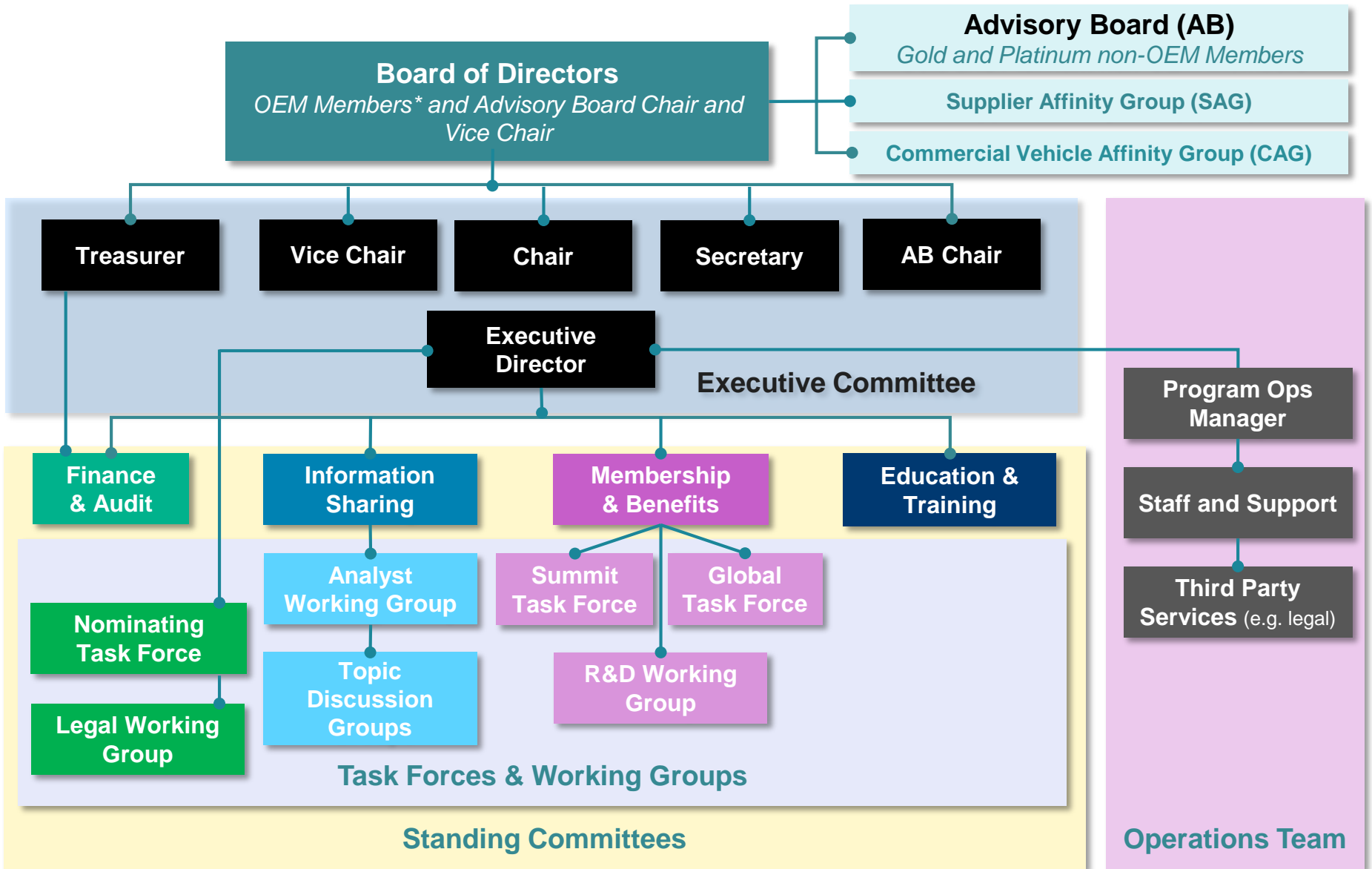
% Taking Educational
Offerings
Maturity Surveys

RELATIONSHIPS

% Member Satisfaction
with value added
relationships

Bottom Line Goal: *Automotive Cybersecure & Resilient Across Industry!*

AUTO-ISAC OPERATING MODEL



2020 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

2020 ADVISORY BOARD (AB) LEADERSHIP



Todd Lawless
*Chair of the
Advisory Board*
Continental



Brian Murray
*Vice Chair of the
Advisory Board*
ZF



Kevin Walker
Chair of the SAG
Aptiv



Larry Hilkene
Chair of the CAG
Cummins

MEMBER ROSTER

AS OF MARCH 19, 2020

Highlighted = new member

Aisin	Hitachi	Oshkosh Corp
Allison Transmission	Honda	PACCAR
Aptiv	Hyundai	Panasonic
AT&T	Infineon	Qualcomm
Blackberry	Intel	Renesas Electronics
BMW Group	Kia	Subaru
Bosch	Knorr Bremse	Sumitomo
Calsonic Kansei	Lear	Tokai Rika
Continental	LGE	Toyota
Cummins	Magna	TuSimple
Denso	Magneti Marelli	Valeo
Delphi Technologies	Mazda	Veoneer
Enterprise Holdings	Mercedes-Benz	Verizon
FCA	Mitsubishi Motors	Volkswagen
Ford	Mitsubishi Electric	Volvo Cars
Garrett	Mobis	Volvo Group
General Motors	Navistar	Waymo
Geotab	Nissan	Yamaha Motors
Google	NXP	ZF
Harman		TOTAL: 58

2020 AUTO-ISAC STAFF

Staff Positions OPEN
 Membership Engagement Lead
 Organization Coordinator



Faye Francy
Executive Director
 fayefrancy@
 automotiveisac.com



Josh Poster
Program Operations Manager
 joshposter@
 automotiveisac.com



Ricky Brooks, II
Intelligence Officer
 rickybrooks@automotiveisac.com



Jake Walker
Cyber Intel Analyst
 jacobwalker@
 automotiveisac.com



Lisa D. Scheffenacker
Business Administrator
 lisascheffenacker@
 automotiveisac.com

**External
 Support
 Staff**



Julie Kirk
Finance
 juliekirk@
 automotiveisac.com



Linda Rhodes
Legal Counsel,
Mayer Brown
 lrhodes@mayerbrown.com



Callen Mackey
CPA,
RSM US LLP
 Callen.mackey@rsmus.com

AUTO-ISAC ACTIVITIES

Auto-ISAC

- **First Quarter New Members:** Renesas, Qualcomm, Google, Oshkosh, Knorr Bremse (Bendix). Please join me in welcoming our new Members!
- **First Quarter New Strategic Partner:** Upstream Security
- **Advisory Board & Board of Directors Meeting Held Virtually March 19**
- **Kevin Tierney, Chair <GM> presented Auto-ISAC 2020 Way Forward**
- **Auto-ISAC TTX going virtual**
- **CyberStorm 2020 postponed**
- **Other events cancelled or postponed: IQPC, TU-Auto, escar**
- **Our next quarter meetings going virtual**

Stay safe, secure and well!

AUTO-ISAC SUMMIT – OCT 14-15

AUTO-ISAC
SUMMIT

2 days

400 attendees



Oct. 14-15,
2020
Detroit, MI

ABOUT THE AUTO-ISAC SUMMIT:

The 2020 Auto-ISAC Summit hosted by General Motors connects global automotive industry insiders during two days of transformative conversations around cyber attack resilience and response.



WHAT'S TRENDING?

Researchers are actively investigating many different attack vectors in modern vehicles

- **Hackers Can Clone Millions of Toyota, Hyundai, and Kia Keys:** Researchers from KU Leuven in Belgium and the University of Birmingham in the UK earlier this week revealed new vulnerabilities they found in the encryption systems used by immobilizers, the radio-enabled devices inside of cars that communicate at close range with a key fob to unlock the car's ignition and allow it to start. ([Link](#))
- **CVE-2020-10558 | Tesla Model 3 Vulnerability:** The driving interface of Tesla Model 3 vehicles in any release before 2020.4.10 allows Denial of Service to occur due to improper process separation, which allows attackers to disable the speedometer, web browser, climate controls, turn signals, navigation, autopilot notifications, and blinker notifications along with other miscellaneous functions from the main screen. This issue is fixed in any release \geq 2020.4.10. ([Link](#))
- **Hacking an Audi: Performing a Man-in-the-Middle Attack on FlexRay:** This medium post is about a project by three comma employees. The goal was to inject steering commands onto the FlexRay bus of an Audi as a proof of concept for adding openpilot support for a FlexRay vehicle. ([Link](#))
- **Turning an OBD-II Reader into a USB / NFC Attack Tool:** Modifying existing software and hardware for an embedded device can be a complex, but rewarding, experience. It can teach valuable development and reverse engineering skills which can be transferred to other aspects of IoT security, and can allow you to breathe new life into your junk. ([Link](#))

For more information or questions please contact analyst@automotiveisac.com

CISA RESOURCE HIGHLIGHTS



CISA
CYBER+INFRASTRUCTURE

Current Activity - Defending Against COVID-19 Cyber Scams

- Serves as a reminder of standard vigilance protocol associated with links and attachments in emails
- Reminds readers to use trusted and verified resources, such as government sites for updates and facts associated with COVID-19
- Reminds readers to verify charity authenticity before making donations (includes link to FTC resource)
- Available for review at <https://www.us-cert.gov/ncas/current-activity/2020/03/06/defending-against-covid-19-cyber-scams>



Activity Alert - AA20-073A – Enterprise VPN Security (TLP: WHITE)

- Activity Alert (AA) intended to provide considerations for enterprise telework requirements as organizations' operational and continuity requirements associated with Covid-19 response include teleworking for their personnel
- Reminds that more vulnerabilities are being found and targeted by malicious cyber actors as telework use increases.
- Delayed patching and inadequate authentication measures in the VPN complex leave entities vulnerable
- Available for review at <https://www.us-cert.gov/ncas/alerts/aa20-073a>
- Feedback and additional information can be provided at CISAServiceDesk@cisa.dhs.gov



Activity Alert - AA20-073A – Enterprise VPN Security (TLP: WHITE) - Continued

- Other Activity Alerts for consideration that we've covered previously:
 - AA20-031A Detecting Citrix CVE-2019-19781 - [https://www\[.\]us-cert \[.\]gov/ncas/alerts/aa20-031a](https://www[.]us-cert[.]gov/ncas/alerts/aa20-031a)
 - AA20-020A Critical Vulnerability in Citrix Application Delivery Controller, Gateway, and SD-WAN WANOP - [https://www\[.\]us-cert\[.\]gov/ncas/alerts/aa20-020a](https://www[.]us-cert[.]gov/ncas/alerts/aa20-020a)
 - AA20-010A Continued Exploitation of Pulse Secure VPN Vulnerability - [https://www\[.\]us-cert\[.\]gov/ncas/alerts/aa20-010a](https://www[.]us-cert[.]gov/ncas/alerts/aa20-010a)



CISA Insights - Risk Management for Novel Coronavirus (COVID-19) (TLP: WHITE)

- Designed to be a resource for executives to help them think through physical, supply chain, and cybersecurity issues that may arise from the spread of Novel Coronavirus, or COVID-19
- Summarizes CISA's role in working with interagency and industry partners
- Provides input on:
 - Actions for Infrastructure Protection
 - Actions for your Supply Chain
 - Cybersecurity for Organizations
 - Cybersecurity Actions for your Workforce and Consumers
 - Download from
[https://www\[.\]cisa\[.\]gov/sites/default/files/publications/20_03_18_cisa_insights_coronavirus.pdf](https://www[.]cisa[.]gov/sites/default/files/publications/20_03_18_cisa_insights_coronavirus.pdf)



CISA Guidance on the Essential Critical Infrastructure Workforce(TLP: WHITE)

- Follows the President's issuance of updated Coronavirus Guidance for America that highlighted the importance of the critical infrastructure workforce.
- Includes an advisory list developed by CISA in collaboration with other federal agencies, State and local governments, and the private sector
- Intent of the advisory list is to help State, local, tribal and territorial officials as they work to protect their communities, while ensuring continuity of functions critical to public health and safety, as well as economic and national security.
- This list is advisory in nature. It is not, nor should it be considered, a federal directive or standard.
- Available at [https://www\[.\]cisa\[.\]gov/publication/guidance-essential-critical-infrastructure-workforce](https://www[.]cisa[.]gov/publication/guidance-essential-critical-infrastructure-workforce)



DHS and FEMA COVID-19 Resources

- <https://www.dhs.gov/coronavirus>
- <https://www.cisa.gov/coronavirus>
- <https://www.fema.gov/coronavirus>
- <https://www.fema.gov/news-release/2020/03/13/covid-19-emergency-declaration>



CISA
CYBER+INFRASTRUCTURE



CISA
CYBER+INFRASTRUCTURE

For more information:
cisa.gov

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

COMMUNITY SPEAKER SERIES

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 our Auto-ISAC (staff@automotiveisac.com)

7 *Best Practice Guides available on website*

1900+
Community Participants

25 *Featured Speakers to date*

COMMUNITY SPEAKERS

EXAMPLE OF PREVIOUS COMMUNITY SPEAKERS

- **Urban Jonson**, NMFTA, Heavy Vehicle Cybersecurity Working Group (April 2018)
- **Ross Froat**, American Trucking Association, ATA Cyberwatch Program (Oct 2018)
- **Katherine Hartman**, Chief – Research, Evaluation and Program Management, ITS Joint Program Office, US DOT (August 2019)
- **Joe Fabbre**, Global Technology Director, Green Hills Software (October 2019)
- **Oscar Marcia**, CISSP, Eonti, Device Authentication in Auto-ISAC as a Foundation to Secure Communications (November 2019)
- **Amy Smith**, the Manager of Pre-College Educational Programming at SAE International (January 2020)

Community Call Slides are located at: www.automotiveisac.com/communitycalls/

WELCOME TO TODAY'S SPEAKER

Jason Conley, Executive Director OmniAir Consortium



- **OmniAir Consortium** is the leading industry association promoting interoperability and certification for ITS, tolling, and Connected Vehicles. Mr. Conley has over 15 years of experience in transportation and security technologies.
- Jason has served in senior roles at the Transportation Security Administration, the U.S. Chamber of Commerce, the Intelligent Transportation Society of America, and the shared mobility start-up, Avego (Carma Tech).
- He earned his law degree at the Columbus School of Law at the Catholic University of America, and an undergraduate degree from Wake Forest University.
- Jason is a member of the Virginia State Bar.



®

OMNIAIR

CONSORTIUM

OmniAir Overview
Auto-ISAC Community Meeting
Wednesday, April 1, 2020



Industry Driven by Members (~80, various expertise)



Working Committees:

- Certification Procedures
- Tolling and Payment Services
- DSRC Technology Devices & Testing
- **Cybersecurity (Security and Certificates)**
- 5GAA / C-V2X Technology



Membership Policy



Confidentiality Policy & Certified Products Posting



Intellectual Property (IP) Policy



Trademark Registered & Policy

OMNIAIR ECOSYSTEM:

- Automotive OEMs
- Tier One Suppliers
- Chipset & Technology Component Providers
- Cybersecurity
- Tolling Devices
- Systems Integrators
- Deploying Agencies
- Test Tools
- Test Labs
- V2X Devices
- Research Institutes



ASSOCIATE MEMBERS





CERTIFICATION SERVICES

Tolling Certification



Since 2012, OmniAir® has offered certification for RFID tolling tags and readers and single and multi-protocol operations.

Connected Vehicle Certification



Since 2017, OmniAir® has offered certification for DSRC-V2X devices for connected vehicles, including OBUs and RSUs.

Developing C-V2X certification program target launch Q3.

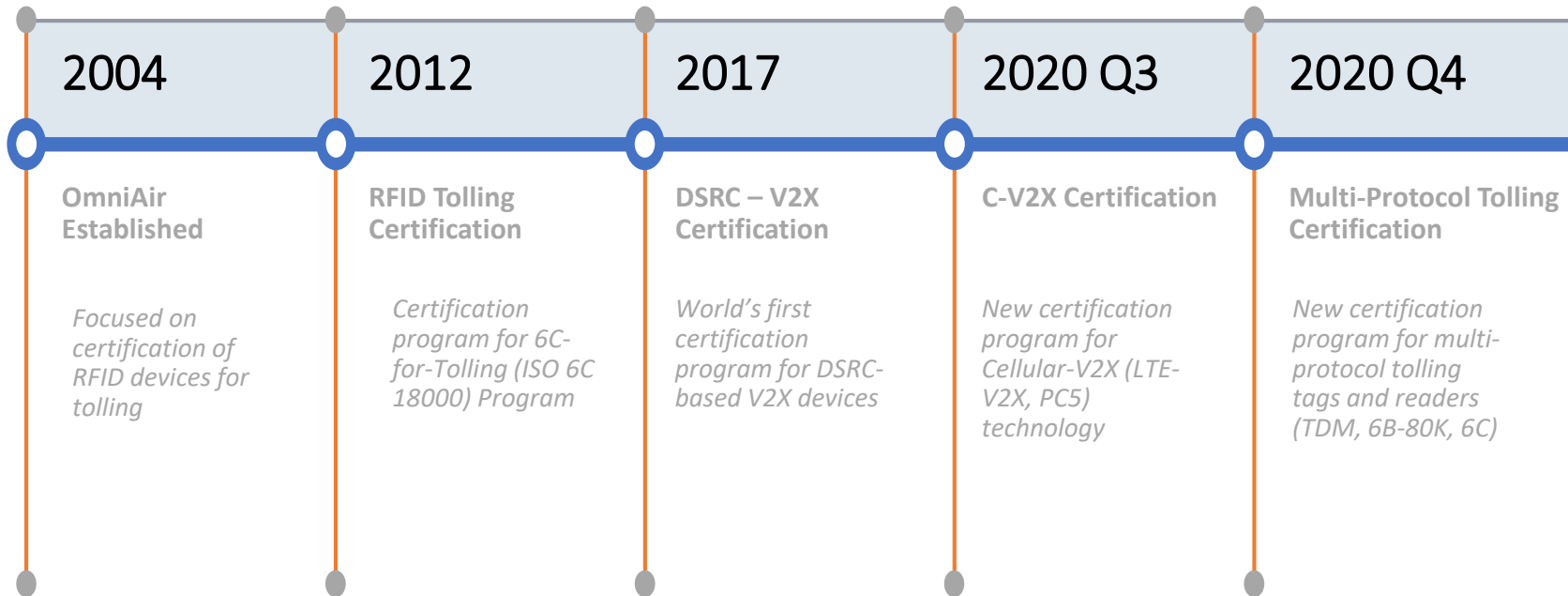
Authorized Test Laboratories



Qualified Test Equipment



OmniAir Certification Programs






Why Certification?

- **Independent, third-party testing by accredited laboratory & test report**
- **Access to Security Credentials to Known Devices**
- **Conformance & Verification per Test Cases of Standards & Specifications**
- **Minimizes Product Variations & Change Requests in Control Releases**
- **Provides Consistency for Device Applications**
- **Ensures Interoperability among Devices**
- **Qualified Device List for Agency Procurement**
- **Environment Control & Inspection (Surveillance)**



Benefits to End-Users of Certification

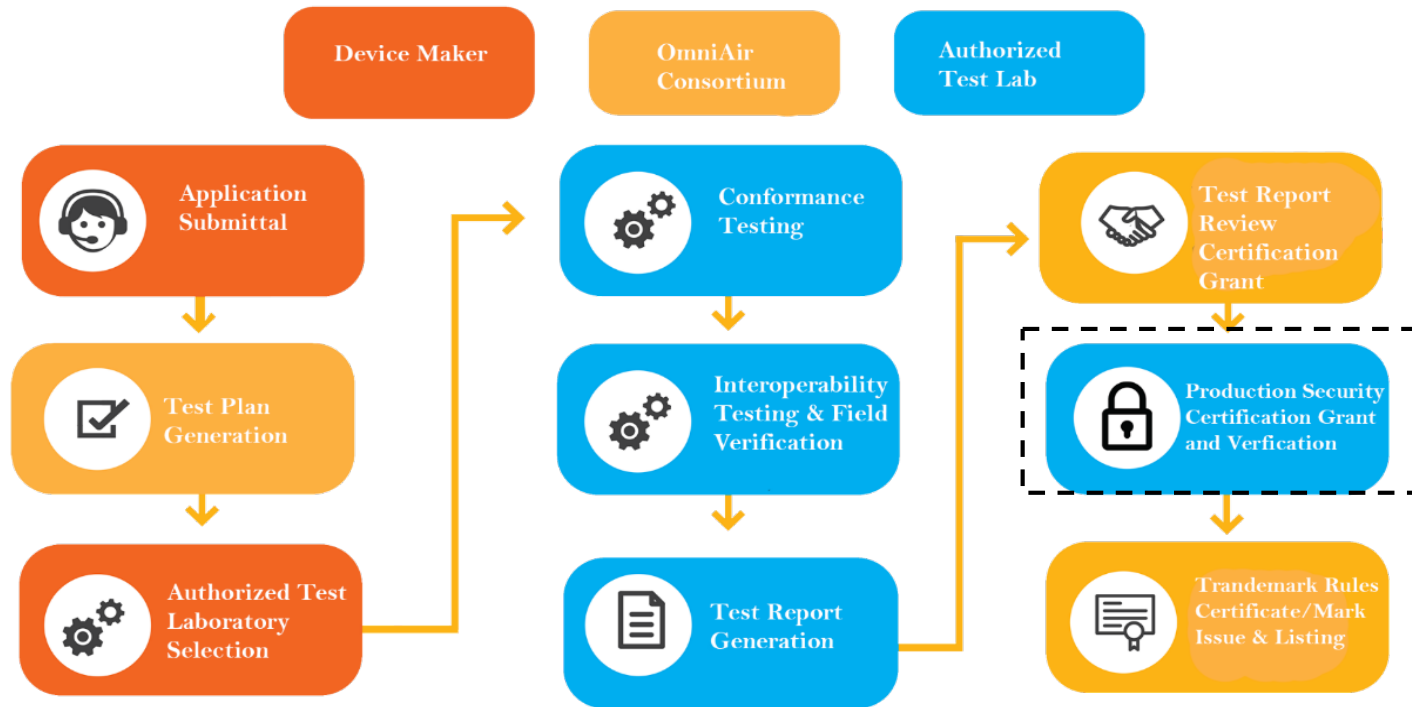
- USDOT Connected Vehicle Pilots first to require OmniAir's device level testing and verification coverage for V2X communication functionality
 - OmniAir process is exposed to many industry devices and their "standards" interpretations and provide conformance, interoperability and consistency platform
 - OmniAir with industry consensus provides "state of the art" interpretation & clarification for certain "sticky" V2X requirements
 - Test Scope covers aspects not easily tested in the field or by vendors themselves
- 

- **Device** tested at **Authorized Test Laboratory (OATL)** with **Qualified Test Equipment (OQTE)** to approved Release scope
- **Certified Devices** does not mean or misconstrued as Reference Devices
- **Reference Device** is separate classification being developed
- **Certification** and **Conformance** is evolving process that requires active industry participation
- **Test Cases** are defined as key element verification but may not cover every element in a standard or specification
- **Surveillance** is key aspect in maintaining device integrity in the environment done at periodically, request or Plugfest basis

What makes
OmniAir's
Certification
Program
Trusted?



Certification Program Elements & Process Flow



CERTIFICATION PROGRAMS



PURPOSE & SCOPE



CERTIFICATION PROCESS



APPLICATION



TESTING



CERTIFICATION PACKAGE REVIEW & DECISION

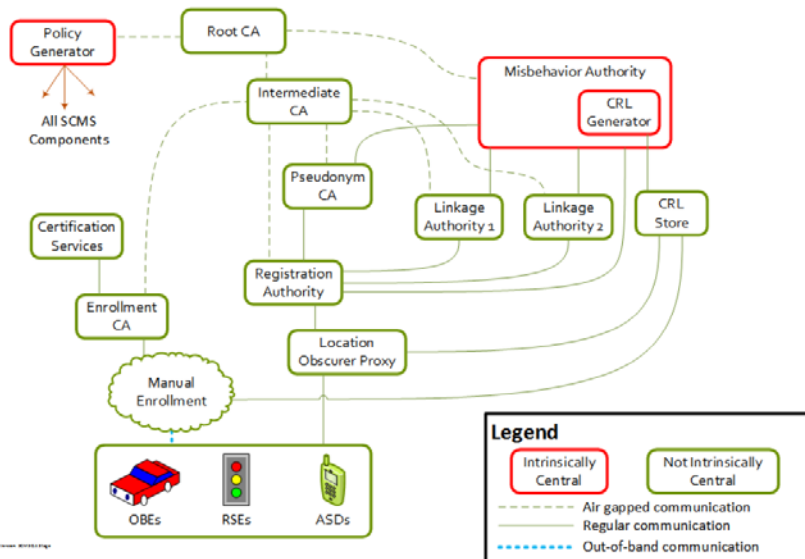


CERTIFICATION MAINTENANCE



SURVEILLANCE

Security Credential Management System (SCMS)



- Originally Developed by USDOT
- IEEE 1609.2.1 Standard in-works
- Expands SCMS is used to enroll devices and provide certificates to Connected Vehicle devices
- Ensure the Confidentiality, Integrity, and Assurance of the Over-The-Air Messages sent and received



Device Test Cases for Security & SMCS

- Starting Test Equipment Automation for SCMS & Expired Test Cases (left)
- Security Minimum Guidelines being Finalization

IEEE 1609.2 Security Services

16092-SPDUBSM-SEND-BV-01	BSM Security Header
16092-SPDUBSM-SEND-BV-02	BSM digitally signed certificate
16092-SPDUBSM-SEND-BV-03	BSM digitally signed digest
16092-SPDUBSM-SEND-BV-04	BSM certificate per vMaxCertDigesInterval
16092-SPDUBSM-SEND-BV-05	BSM digest with valid signature
16092-SPDUBSM-SEND-BV-06	BSM certificate with valid signature
16092-SPDUBSM-RECV-BV-01	IUT acknowledges valid BSM security header.
16092-SPDUBSM-RECV-BV-02	IUT acknowledges valid BSM implicit certificate.
16092-SPDUBSM-RECV-BV-03	IUT acknowledges valid BSM signed digest.
16092-SPDUBSM-RECV-BV-04	IUT acknowledges valid BSM's certificate GenerationTime & Expiration Time
16092-SPDUBSM-RECV-BV-05	IUT acknowledges BSM's Digest GenerationTime & Expiration Time
16092-SPDUBSM-CERTCHG-BV-01	BSM's vCertChangeInterval Changes
16092-SPDUBSM-RECV-BI-01	IUT acknowledges invalid BSM with incorrect digest signature.
16092-SPDUBSM-RECV-BI-02	IUT acknowledges invalid BSM with incorrect certificate signature.
16092-SPDUWSA-SEND-BV-01	IUT generates correct WSA security header.
16092-SPDUWSA-SEND-BV-02	IUT generates correct WSA certificate data structure.
16092-SPDUWSA-SEND-BV-04	IUT generates WSA's Signed Certificate & Signature
16092-SPDUWSA-RECV-BV-01	IUT acknowledge valid WSA security header.
16092-SPDUWSA-RECV-BV-02	IUT acknowledges valid implicit certificate signed WSA.
16092-SPDUWSA-RECV-BI-01	IUT acknowledges invalid WSA w/incorrect cert signature & not transmit.

SCMS V0 Testing - Approved for Implementation

TP ID	Description
TP-CAMP-SCMS-SEND-BV-01	Validate that the IUT's file system has all required information needed for bootstrapping process
TP-CAMP-SCMS-SEND-BV-02	Validate that the IUT will request Application certificates in legitimate form
TP-CAMP-SCMS-SEND-BV-03	Validate that the IUT will request Pseudonym certificates in legitimate form
TP-CAMP-SCMS-RECV-BV-01	Validate that the IUT can receive Application certificate from the RA
TP-CAMP-SCMS-RECV-BV-02	Validate that the IUT can receive Pseudonym certificate from the RA

1609.2 Testing – Approved for Implementation

TP ID	Description
TP-16092-EXPCERT-BV-01	Validate that the IUT will reject loading expired certificate bundles into certificate storage
TP-16092-EXPCERT-SEND-BV-01	Validate that the IUT will not transmit SPDUs once Root certificate expires
TP-16092-EXPCERT-SEND-BV-02	Validate that the IUT will not transmit SPDUs once intermediate certificate expires
TP-16092-EXPCERT-SEND-BV-03	Validate that the IUT will not transmit BSMs once pseudonym certificate expires
TP-16092-EXPCERT-RECV-BV-01	Validate that the IUT will not receive SPDUs once Root certificate expires
TP-16092-EXPCERT-RECV-BV-02	Validate that the IUT will not receive SPDUs once intermediate certificate expires
TP-16092-EXPCERT-RECV-BV-03	Validate that the IUT will not receive SPDUs once pseudonym certificate expires
TP-CYBERSEC-SECPROF-RECV-BV-01	Validate that the IUT will reject repeat BSM messages



Active Participation from leading SCMS Providers:

- Autocrypt – South Korea
- Blackberry – Canada
- ESCRYPT – Canada
- Green Hills / ISS – United States

Cybersecurity Working Group: Next Steps

In the Works:

- Field Testing for Multiple Source Certificate Interoperability
- SCMS interaction testing based on the new IEEE 1609.2.1 standard in the works
- Expanding Security Profile Testing

Future Considerations:

- Certificate Revocation List (BSM Misbehavior)
- Testing per new CEN / ISO TC 21186
- Testing per new ISO TC 21177
- Service Specific Permissions (SSP) testing



OmniAir Plugfest Device Testing



Contact us



Jason M. Conley
Executive Director

O: 202-503-1421
M: 202-441-9313
jconley@omniair.org
www.omniair.org

1250 Connecticut Ave., NW
8th Floor, Suite 825
Washington, DC 20036

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 COMPANY, NOW IS A GREAT TIME TO JOIN 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 Staff (staff@automotiveisac.com).

STRATEGIC PARTNERSHIP PROGRAMS

Solutions Providers

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

Examples: Hacker ONE, SANS, IOActive

Associations

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

Examples: Auto Alliance, Global Auto, ATA

Affiliations

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

Examples: NCI, DHS, NHTSA

Community

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

Examples: Summit sponsorship – key events

INNOVATOR

Paid Partnership

- Annual investment and agreement
- Specific commitment to engage with ISAC
- In-kind contributions allowed

NAVIGATOR

Support Partnership

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

COLLABORATOR

Coordination Partnership

- “See something, say something”
- May not require a formal agreement
- Information exchanges- coordination activities

BENEFACTOR

Sponsorship Partnership

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

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

Josh Poster
Program Operations
Manager



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



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