Welcome to Auto-ISAC!

Monthly Virtual Community Call

November 4, 2020

Agenda

Time (ET)	Topic
11:00	**Welcome** ➢ Why We're Here ➢ Expectations for This Community
11:05	**Auto-ISAC Update** ➢ Auto-ISAC Activities – *the Summit* ➢ Heard Around the Community ➢ What's Trending
11:15	***DHS CISA Community Update***
11:20	**Featured Speaker: Kiersten Todt**, Cyber Readiness Institute (CRI), Managing Director
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! (lisascheffenacker@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*

12 *Innovator Partners*

❖ Participate

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

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

36 *Supplier & Commercial Vehicle Members*

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

Coordination with **26** *critical infrastructure ISACs through the National Council of ISACs (NCI)*

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

Chris Lupini
Chair of the SAG
Aptiv

Larry Hilkene
Chair of the CAG
Cummins

Member Roster

As of November 4, 2020

Highlighted = Change

Aisin	Honda	Oshkosh Corp
Allison Transmission	Hyundai	PACCAR
Aptiv	Infineon	Panasonic
AT&T	Intel	Qualcomm
Blackberry Limited	Kia	Renesas Electronics
BMW Group	Knorr Bremse	Subaru
Bosch	Lear	Sumitomo Electric
Continental	LGE	Tokai Rika
Cummins	Magna	Toyota
Delphi Technologies	MARELLI	TuSimple
Denso	Mazda	Valeo
FCA	Mercedes-Benz	Veoneer
Ford	Mitsubishi Motors	Volkswagen
Garrett	Mitsubishi Electric	Volvo Cars
General Motors	Mobis	Volvo Group
Geotab	Navistar	Waymo
Google	Nexteer Automotive Corp	Yamaha Motors
Harman	Nissan	ZF
Hitachi	NXP	TOTAL: 56

Auto-ISAC Activities

➢ Auto-ISAC Virtual Summit Oct 14-15 – Completed

1. We'd love to hear your impressions on our first virtual summit.
2. Please provide any feedback to Sharmila Khadka – sharmilakhadka@automotiveisac.com

➢ Other Key Auto-ISAC Member Events -

1. Member Survey OPEN: Nov 3-13
2. ETSC Event:
   a) Tuesday, November 19, Aptiv presenting on: *"Risk Assessment Methodology for 21434 Compliance".*
   b) Wednesday, December 9 presentation by T. Gaertner (BMW) *"Security Testing".*
3. All Member's Meeting: Wednesday, Dec 2nd 1-3 pm
4. Advisory Board Meetings: Thursday, Dec 3rd, 9-12 pm
5. Board of Directors Meeting: Thursday, Dec 3rd, 2-4 pm

2020 Summit Feedback Received

HUGE Summit content. Flawless execution.

Congratulations on the event, overall it appeared to be very successful.

Really great summit overall, well done and congratulations to the organizers and presenters!

Thank you for creating a compelling conference with both theoretical and actionable insights. The online platform was among the easiest I have used for online conferences, so kudos for selecting a good system.

Congratulations on the successful virtual summit and thank you so much for putting together a great informatic summit for us to benefit from as a member.

Actually really enjoyed the virtual format. Recommend going both ways in the future.

Not all can break away for in person events, but the virtual format was very helpful.

The experience was rather unique, considering all the challenges of being virtual. However, the effort on the part of the organizers and speakers showed throughout the conference. The speakers/sessions managed time extremely well. The experience was seamless with minimal disruption/technical difficulties. Kudos to the team!

Auto-ISAC Intelligence

What's Trending?

- ***The Auto-ISAC assesses the US Government has taken steps to dissuade foreign powers from interfering in US elections.***

- ***Recent statements made by US agencies provide valuable information for defenders to ensure that they are sufficiently protected against similar TTPs as those highlighted in recent products, indictments, and statements.***

- ***Ransomware has posed a significant threat to critical infrastructure. Ryuk is especially dangerous, as highlighted below.***

US Treasury Sanctions Russian Research Institute Behind Triton Malware

Sanctions were levied today against the State Research Center of the Russian Federation FGUP Central Scientific Research Institute of Chemistry and Mechanics (also known as CNIIHM or TsNIIKhM). A FireEye report published in October 2018 identified CNIIHM as the possible author of the Triton malware. Researchers said Triton contained instructions that could either shut down a production process or allow SIS-controlled machinery to work in an unsafe state, creating a risk of explosions and risk to human operators and their lives.

Ryuk in 5 Hours

The Ryuk threat actors went from a phishing email to domain wide ransomware in 5 hours. They escalated privileges using Zerologon (CVE-2020-1472), less than 2 hours after the initial phish. They used tools such as Cobalt Strike, AdFind, WMI, and PowerShell to accomplish their objective.

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

CISA RESOURCE HIGHLIGHTS

TLP:WHITE DHS Homeland Threat Assessment

- **Released by DHS on October 6, 2020**
  - **The DHS Homeland Threat Assessment (HTA) provides a summary of the following threats:**
  - **Cyber**
  - **Foreign Influence Activity**
  - **Economic Security**
  - **Terrorism**
  - **Transnational Criminal Organization**
  - **Illegal Immigration**
  - **Natural Disasters**
- **Available for download at:**
  - **https://www[.]dhs[.]gov/sites/default/files/publications/2020_10_06_homeland-threat-assessment.pdf**

CISA Telework Essentials Toolkit – Chapter 5

- **Focus on strategies for cultivating a data protection culture to ensure data confidentiality, integrity and accessibility (CIA)**
- **Includes links to resources for backup management strategies, and safeguards against ransomware, malware, and other attacks**
- **All five (5) chapters can be individually downloaded in PDF format from https://www[.]cisa[.]gov/publication/cyber-essentials-toolkits**

TLP: WHITE – Activity Alert AA20-304A - Iranian Advanced Persistent Threat Actor Identified Obtaining Voter Registration Data

- **Co-authored by CISA and the FBI, providing awareness of an Iranian advanced persistent threat (APT) actor targeting U.S. state websites—to include election websites**
- **The actor is assessed to be responsible for the mass dissemination of voter intimidation emails to U.S. citizens and the dissemination of U.S. election-related disinformation in mid-October 2020**
- **AA20-304A includes technical details, including indicators of compromise (IOCs)**
- **AA20-304A and FBI FLASH ME-000138TT available for review at:**
  - **https://us-cert[.]cisa[.]gov/ncas/alerts/aa20-304a**
  - **https://www[.]ic3[.]gov/Media/News/2020/201030.pdf**

TLP: WHITE – Activity Alert (AA20-296B)
Iranian Advanced Persistent Threat Actors Threaten Election-Related Systems

- **CISA and FBI warn that Iranian APT actors are likely intent on influencing and interfering with the U.S. elections to sow discord among voters and undermine public confidence in the U.S. electoral process**
- **The APT actors have historically exploited critical vulnerabilities to conduct DDoS attacks, SQL injections attacks, spear-phishing campaigns, website defacements, and disinformation campaigns.**
- **AA20-296B includes technical details about these types of attacks, mitigation strategies, and additional CISA resources**
- **Available for review at https://us-cert[.]cisa[.]gov/ncas/alerts/aa20-296b**

TLP:WHITE CISA Activity Alert AA20-301A - North Korean Advanced Persistent Threat Focus: Kimsuky

- **Result of result of analytic efforts between the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI) and the Cyber National Mission Force (CNMF)**
- **AA20-301A describes tactics, techniques and procedures (TTPs) used by the North Korean APT threat actor Kimsuky**
- **Likely tasked by the North Korean regime for a global intelligence gathering mission**
- **TTPs include social engineering, spearphishing, and wateringhole attacks**
- **Details available at:**
  - **https://us-cert[.]cisa[.]gov/ncas/alerts/aa20-301a**
  - **https://www[.]us-cert[.]cisa.gov/northkorea**

TLP: WHITE – CISA Analysis Report AR20-303B/Malware Analysis Report (MAR) – 10310246-1.v1 – Zebrocy Backdoor

- **Result of result of analytic efforts between the Cybersecurity and Infrastructure Security Agency (CISA) and the Cyber National Mission Force (CNMF)**
- **2 samples submitted - 32-bit windows executables written in the Golang programming language**
- **Samples identified as new variants of the Zebrocy backdoor**
- **Analysis details, security posture best practices, and indicators of compromise (IOCs) available at:**
  - **https://us-cert[.]cisa[.]gov/ncas/analysis-reports/ar20-303b**
  - **https://us-cert[.]cisa[.]gov/sites/default/files/publications/MAR-10310246-1.v1.WHITE.stix.xml**

TLP: WHITE – CISA Analysis Report AR20-303A/Malware Analysis Report (MAR) – 10310246-2.v1 – PowerShell Script: ComRAT

- **Result of result of analytic efforts between CISA, CNMF, and FBI**
- **ComRAT seen to be used by Russian APT group Turla. Thought to be the threat actor in this instance of ComRAT's use.**
- **MAR analyzes a PowerShell script that installs a PowerShell script that decodes and loads a 64-bit DLL identified as ComRAT version 4 that includes communications modules**
- **Analysis details and IOCs available at:**
  - **https://us-cert[.]cisa[.]gov/ncas/analysis-reports/ar20-303ba**
  - **https://us-cert[.]cisa[.]gov/sites/default/files/publications/MAR-10310246-2.v1.WHITE.stix.xml**

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

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

7 ***Best Practice Guides available on website***

2000+
Community Participants

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!

Slides available on our website – www.automotiveisac.com

Featured Speaker

AUTO-ISAC
Automotive Information Sharing and Analysis Center

Kiersten Todt, Cyber Readiness Institute

Managing Director- CRI

Kiersten Todt currently serves as the Managing Director of the Cyber Readiness Institute (CRI), a non-profit initiative that convenes senior executives of global companies to develop free cybersecurity tools and resources for small businesses, worldwide. She founded CRI in 2017 with the CEOs of Mastercard, Microsoft, PSP Partners, and the retired CEO of IBM.

Ms. Todt also advises senior executives and Boards on cyber risk management and the role of human behavior in cybersecurity. She most recently served as Executive Director of the U.S. Presidential Commission on Enhancing National Cybersecurity and has served in senior positions in the White House and United States Senate, where she drafted components of the legislation to create the U.S. Department of Homeland Security.

Ms. Todt has commented on national security and cybersecurity issues in multiple media outlets, including NBC, CBS, NPR, Bloomberg, CNN, FoxNews, The New York Times, The Wall Street Journal, and The Washington Post. Her writing on national security and cybersecurity has been published in relevant journals and news publications.

CYBER READINESS
INSTITUTE

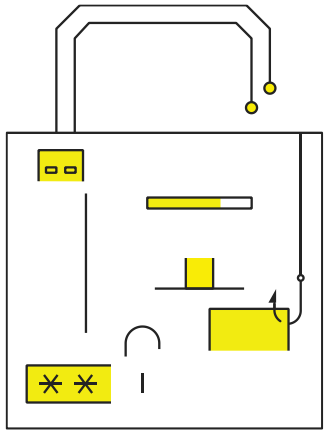
Helping Your Business Become Cyber Ready

Kiersten Todt
Managing Director, The Cyber Readiness Institute

November 4, 2020

Current Cybersecurity Environment and Risks

- According to Brian Moynihan, CEO, Bank of America, 80% of businesses have less than 10 employees and 95% have less than 100 employees (*Face the Nation*, April 26, 2020).
- According to the SBA Administrator, every hour another small business is closing during the pandemic (*Meet the Press*, April 26, 2020).
- 67% of SMBs fail to survive a cyber breach. (Source: Trustwave)
- 56% organizations suffered a breach caused by a 3rd party. (Source: Trustwave)
- $3.92M is the average cost of a data breach. (Source: Trustwave)



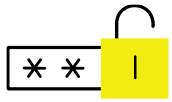
The Cyber Readiness Institute

- Convenes senior leaders of global companies and value chain partners
- Shares cybersecurity best practices and resources
- Develops *free* content and tools to improve cyber readiness of small and medium-sized enterprises

The CRI Approach

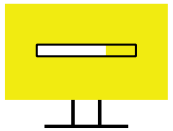
- Focus on human behavior: authentication, patching, phishing, and USB use
- Incident response and resilience
- Guidance and tools on preventative measures and practical incident responses (www.BeCyberReady.com)
    - Cyber Readiness Program
    - Remote Work Resources
- Create a “cyber readiness culture”
- Cyber Leader drives execution
- Small Business Advisory Group provides input

Focus on Four Core Issues for Culture Change



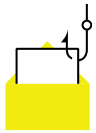
Passwords

- 80% of data breaches could be prevented by using two-factor authentication
- 17% of people use their favorite sports team and the current year as their password.



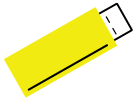
Software Updates

- 77% of attacks in 2017 took advantage of vulnerabilities in the software already on your computers



Phishing

- 91% of all cyber attacks start with a phishing email.
- 81% of companies that fell for a phishing attack lost customers.



USBs

- 8 out of 10 companies' employees use non-encrypted USB devices, such as free USBs from conferences.

The “Core Four”

- **Authentication**
  - Use a pass*phrase* not a pass*word*.
  - Enable multi-factor authentication.
- **Patching**
  - Turn on auto-updates.
- **Phishing**
  - Be suspicious and alert – hover over sender’s name to verify email address.
  - Conduct routine phishing tests.
- **USB Use**
  - Avoid using USBs – instead, use online file sharing or the Cloud.

The Cyber Readiness Program: 5 Stages

- **Get Started:** Prepare organization and select Cyber Readiness Leader.
- **Assess & Prioritize:** Learn about four key issues: Authentication, Patching, Phishing, and USB use. Prioritize what to protect. Establish baseline metrics.
- **Agree & Commit:** Access and modify policy templates so they are practical for organization. Develop incident response plan from template.
- **Roll Out:** Introduce the Cyber Readiness Program to workforce. Access training and communication kit and distribute workforce commitment letter.
- **Measure Success:** Re-do baseline metrics to measure impact. Earn certificate from the Cyber Readiness Institute. [Cyber Leader certification in development.]

Human Behavior: Key to Security

- Cyber readiness is about people and their behavior
- Goals:
  - Embed cyber readiness in how each person does their job
  - Develop good cyber habits
  - Create a culture of cyber readiness in the organization
- Cybersecurity policies need to be as practical as possible

Creating Practical Policies

- Ensure employees understand why cyber readiness is important and why they need to be involved
- Involve employees in developing the policies so they are practical to implement
- Develop policies that are easily accessible and well-communicated

Global Case Studies

- **Corporate HQ of Global Dining Company:** Create culture of cyber readiness
- **Healthcare company:** Modify passphrase
- **Auto Industry:** Secure franchises/brand and reputation
- **State and City Governments:** Onboarding employees and small business support
- **Telecommunications:** Integrate content into supply chain offerings

"For health and safety reasons, we'll be transitioning to cyber crime."

Remote Work Resources

- *Securing a Remote Workforce*
- *Making Your Remote Workforce Cyber Ready*
- *Data Protection Basics for Remote Workers*
- *Creating a Cyber Ready Culture in Your Remote Workforce: 5 Tips*
- *Ransomware Playbook (developed in collaboration with the Department of Homeland Security/CISA)*
- *Cloud FAQ*
- *Top Three Dos and Don’ts for Remote Workers*
- *Keeping Educators and Students Safe*
- *Hybrid Remote-Office Workplace*

Remote Workforce: Top Three Do's & Don'ts

Do

- Use separate passwords/passphrases for work and personal
- Update all software on all devices
- Use Multi-factor Authentication

Don't

- Click on links or attachments in emails
- Send your passwords or bank info by email
- Use USBs, public computers or Wi-Fi if possible

CYBER READINESS
INSTITUTE

Thank You!

Visit us at **becyberready.com**

LinkedIn **@cyber-readiness-institute**

Twitter **@Cyber_Readiness**

Facebook **@CyberReadinessInstitute**

Email at **ktodt@cyberreadinessinstitute.org**

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 Partners

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

[redacted]

INNOVATOR
Strategic Partnership (12)

ArmorText

Celerium

Cybellum

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

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

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

Our contact info

Faye Francy
Executive Director

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

Sharmila Khadka
Executive Organizational Secretary

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