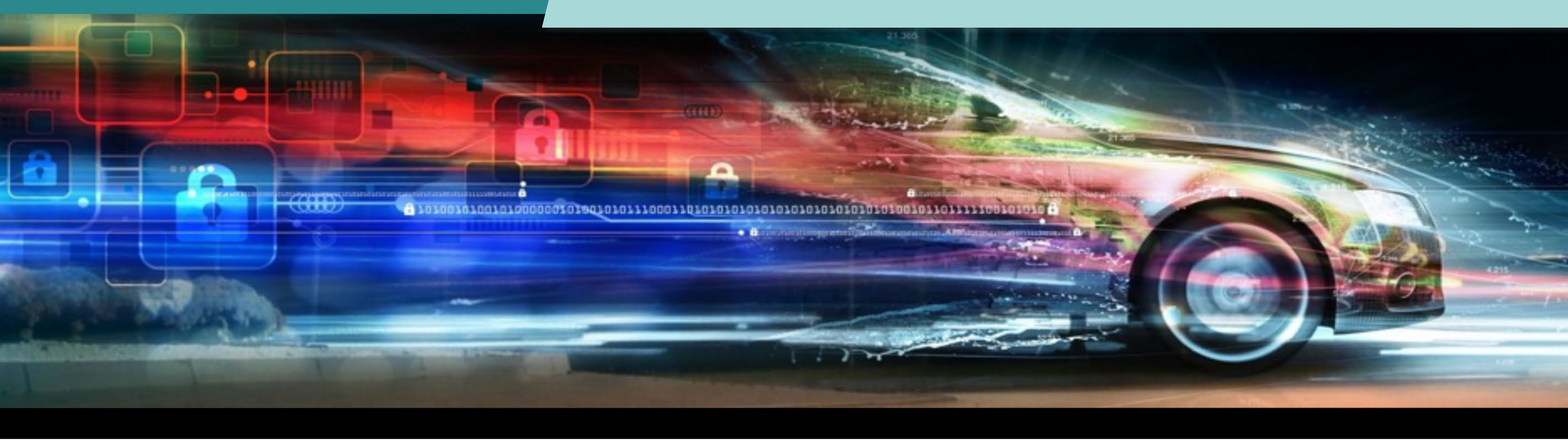


Welcome to Auto-ISAC!

Monthly Virtual Community Call

July 6, 2022

This Session will be recorded.

TLP:WHITE

AUTO-ISAC
Automotive Information Sharing and Analysis Center

DHS Traffic Light Protocol (TLP) Chart

COLOR	WHEN SHOULD IT BE USED?	HOW MAY IT BE SHARED?
TLP:RED 🔴 ⚫ ⚫ Not for disclosure, restricted to participants only.	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.
TLP:AMBER ⚫ 🟡 ⚫ Limited disclosure, restricted to participants organizations.	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.	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.
TLP:GREEN ⚫ ⚫ 🟢 Limited disclosure, restricted to the community.	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.	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.
TLP:WHITE ⚪ ⚪ ⚪ Disclosure is not limited.	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.	Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

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

Agenda

Time (ET)	Topic
11:00	**Welcome** ➢ Why We're Here ➢ Expectations for This Community
11:05	**Auto-ISAC Update** ➢ Auto-ISAC Activities ➢ Heard Around the Community ➢ What's Trending
11:15	***DHS CISA Community Update***
11:20	**Featured Speaker:** ▪ **Bruce Churchill, InfraGard & Stephanie Scheuermann, Ford** ▪ **Title: "The FBI's InfraGard Program"**
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

43 *Supplier & Commercial Vehicle Members*

17 *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)*

2022 - 2023 Board of Directors

Executive Committee (ExCom)

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

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

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

2022-2023 Advisory Board (AB) Leadership

Todd Lawless
Chair *of the*
Advisory Board
Continental

Bob Kaster
Vice Chair *of the*
Advisory Board
Bosch

Allen Houck
Chair *of the SAG*
NXP

Larry Hilkene
Chair *of the CAG*
Cummins

Member Roster
As of July 1, 2022

Highlight = Change

68 Members, 5 in Progress

Aisin	Honda	Nissan	Yamaha Motors
Allison Transmission	Hyundai	Nuro	ZF
Aptiv	Infineon	NXP	
Argo AI, LLC	Intel	Oshkosh Corp	
AT&T	John Deere Electronic	PACCAR	
AVL List GmbH	Kia	Panasonic	
Blackberry Limited	Knorr Bremse	Polaris	
BMW Group	Lear	Qualcomm	
BorgWarner	LGE	Renesas Electronics	
Bosch (Escrypt-Affiliate)	Lucid Motors	Stellantis	
Canoo	Luminar	Subaru	
Continental (Argus-Affiliate)	Magna	Sumitomo Electric	
Cummins	MARELLI	Tokai Rika	
Denso	Mazda	Toyota	
EFS	Mercedes-Benz	TuSimple	
Faurecia	Meritor	Valeo	
Ford	Mitsubishi Motors	Veoneer	
Garrett	Mitsubishi Electric	Vitesco	
General Motors (Cruise-Affiliate)	Mobis	Volkswagen	
Geotab	Motional	Volvo Cars	
Harman	Navistar	Volvo Group	
Hitachi	Nexteer Automotive Corp	Waymo	

Upcoming Events

- **Upcoming Meetings**
  - **Community Call:**
    - **Wednesday, August 3 – Speaker: Gilad Bandel, Cymotive Title: "Lesson Learned from IT and OT ICS/SCADA Cybersecurity Applied to Automotive" Time: *11 – 12:00 p.m.* TLP:WHITE**
  - **Joint AWG & IT/OT Workshop: Tuesday, September 6th 9 a.m. - 4 p.m. at the Henry in Dearborn, MI. Click here for registration. TLP:AMBER**
  - **Members Teaching Members:**
    - **Wednesday, July 20 Speaker: Larry Hilkene, Cummins et al. Title: *J1939 Update* Time: *10 – 11:30 a.m.* TLP:AMBER**
- **Announcements**
  - **Auto-ISAC Cybersecurity Summit** – *Registration is Open!* Both in-person and virtual venue. Dates: September 7-8, 2022 in Dearborn, MI at The Henry Hotel. Your Company PoC has the "free passes" please check with them!

2022 AUTO-ISAC CYBERSECURITY SUMMIT

DRIVING A SECURE FUTURE

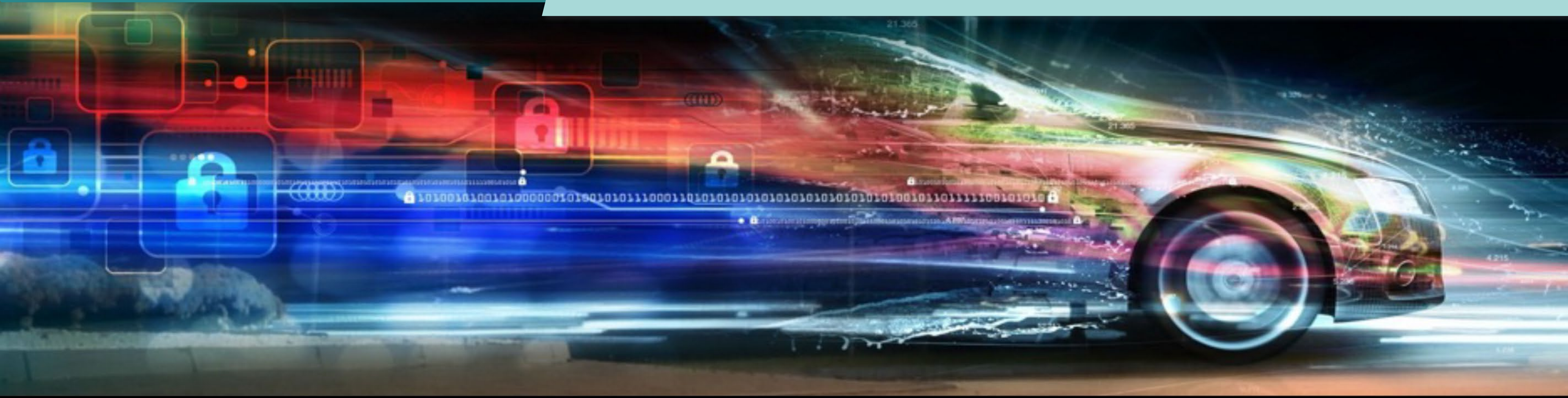
Hybrid Event • Dearborn, MI and Virtual • September 7-8, 2022

AUTO-ISAC
Automotive Information Sharing and Analysis Center

More information here

EVENT HOST & TITANIUM SPONSOR

BOSCH escrypt



Auto-ISAC Intelligence

TLP:WHITE

AUTO-ISAC
Automotive Information Sharing and Analysis Center

Auto-ISAC Intelligence

- Know what we track daily: subscribe to the DRIVEN; know our strategic view of the cyber threat environment: read the TLP:GREEN Threat Assessment in our 2021 Annual Report
  - Send feedback, contributions, or questions to analyst@automotiveisac.com
- Intelligence Spotlight – LockBit vs Mandiant: Potential Implications to Operations
  - On June 6, the LockBit ransomware group published a new page on its dark web site stating it would leak 356,841 files allegedly stolen from Mandiant. Mandiant responded to LockBit's claim stating, "Mandiant is aware of these LockBit-associated claims. At this point, we do not have any evidence to support their claims. We will continue to monitor the situation as it develops."
  - Mandiant later stated it had, "reviewed the data disclosed in the initial LockBit release. Based on the data that has been released, there are no indications that Mandiant data has been disclosed but rather the actor appears to be trying to disprove Mandiant's June 2nd, 2022 research blog on UNC2165 and LockBit." .
  - Though the incident appears to have been a hoax perpetrated by LockBit, reporting indicates Mandiant pivoted to an incident response posture to verify the claim.
  - With limited personnel, pivoting to incident response can detract from normal operations, moving personnel from 'watching the wire' and potentially leaving systems less monitored
  - The Auto-ISAC encourages community member companies to ensure incident response plans do not detract from your ability to continuously monitor and safeguard systems. Threat actors may use similar tactics to open opportunities for attack

CISA RESOURCE HIGHLIGHTS

Case Study: Mozilla Addresses Vulnerabilities

Regardless of industry, service providers need to monitor threats.

Mozilla has released security updates to address vulnerabilities in Firefox, Firefox ESR, and Thunderbird. An attacker could exploit some of these vulnerabilities to take control of an affected system.

Read more here: Mozilla Releases Security Updates for Firefox, Firefox ESR, and Thunderbird | CISA

Think about it: What are potential cyber threats to your organization today?

2022 CWE Top 25 Most Dangerous Software Weaknesses

Understanding software weaknesses ahead of time can enable your organization to be better prepared during crises.

Study the Software Weakness List

The Homeland Security Systems Engineering and Development Institute has released the 2022 Common Weakness Enumeration (CWE) Top 25 Most Dangerous Software Weaknesses list.

Understand the Data

The list uses data from the National Vulnerability Database to compile the most frequent and critical errors that can lead to serious vulnerabilities in software.

Predict Your Attacker's Actions

An attacker can often exploit these vulnerabilities to take control of an affected system, obtain sensitive information, or cause a denial-of-service condition.

2022 CWE Top 25 Most Dangerous Software Weaknesses | CISA

Case Study: Citrix Addresses Vulnerabilities

Regardless of industry, service providers need to monitor threats.

Citrix has released security updates to address vulnerabilities that could affect Hypervisor. An attacker could exploit one of these vulnerabilities to take control of an affected system.

Read more here: Citrix Releases Security Updates for Hypervisor | CISA

Think about it: What are potential cyber threats to your organization today?

Log4Shell Exploitation in VMware Horizon

Log4Shell has threatened and exploited organizations across the country, regardless of industry. Some of the greatest exploitations have resulted in financial, human resource, and other losses.

CISA and USCG have issued warnings.

CISA and the United States Coast Guard Cyber Command (CGCYBER) have released a joint Cybersecurity Advisory (CSA) to warn network defenders that cyber threat actors have continued to exploit CVE-2021-44228 (Log4Shell) in VMware Horizon® and Unified Access Gateway (UAG) servers to obtain initial access to organizations that did not apply available patches.

We want to help you fight this vulnerability.

The CSA provides information—including tactics, techniques, and procedures and indicators of compromise—derived from two related incident response engagements and malware analysis of samples discovered on the victims' networks.

Read more here: Malicious Cyber Actors Continue to Exploit Log4Shell in VMware Horizon Systems | CISA

KEVs Catalog

CISA strongly urges all organizations to reduce their exposure to cyberattacks by prioritizing timely remediation of Catalog vulnerabilities as part of their vulnerability management practice.

CISA has added 49 new vulnerabilities to its Known Exploited Vulnerabilities Catalog in the month of June. These types of vulnerabilities are a frequent attack vector for malicious cyber actors and pose significant risk to the federal enterprise.

Additional Resources from CISA

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

For more information:
cisa.gov

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

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA

Auto-ISAC Community Meeting

Why Do We Feature Speakers?

- These calls are an opportunity for information exchange & learning
- Goal is to educate & provide awareness around cybersecurity for the *connected vehicle*

What Does it Mean to Be Featured?

- Perspectives across our ecosystem are shared from Members, government, academia, researchers, industry, associations and others.
- Goal is to showcase a rich & balanced variety of topics and viewpoints
- *Featured speakers are not endorsed by Auto-ISAC nor do the speakers speak on behalf of Auto-ISAC*

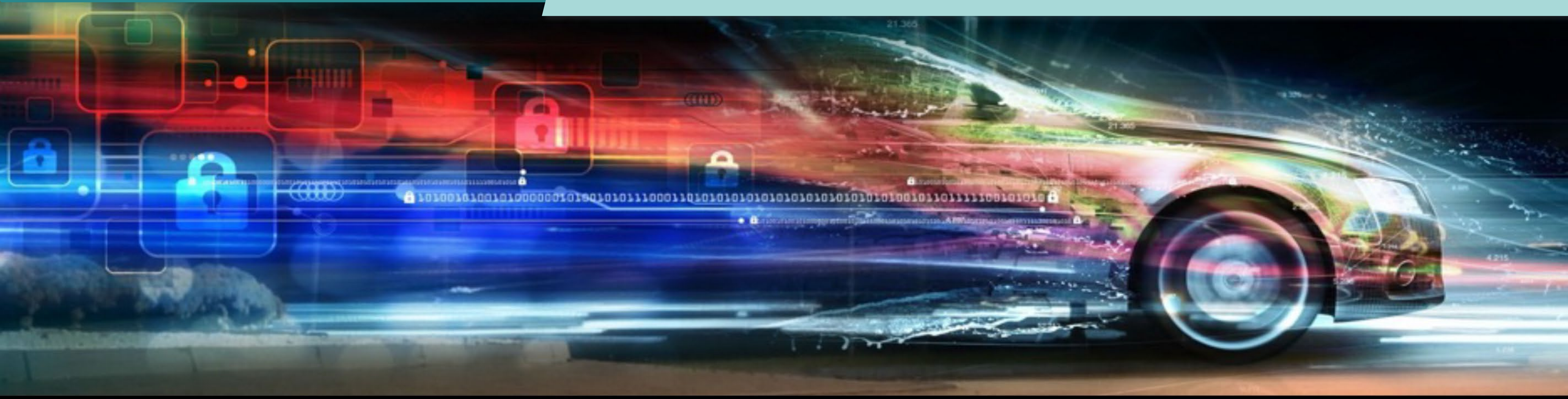
30+ *Featured Speakers to date*

How Can I Be Featured?

- If you have a topic of interest you would like to share with the broader Auto-ISAC Community, then we encourage you to contact us!

7 *Best Practice Guides available on website*

2000+ *Community Participants*



Featured Speaker

TLP:WHITE

AUTO-ISAC
Automotive Information Sharing and Analysis Center

Stephanie Scheuermann, Ford Motor Company

Manager, Data Protection Services

Ms. Scheuermann has served on the board of the MI-IMA six years, in various executive board roles including Secretary, President and now Chairman actively contributing to the chapter for over 8 years.

She has worked at Ford Motor Company for since 1996. Since 2004 she has dedicated her time to building a precision global cyber-incident response team which has resulted in the evolution of three core service areas; Incident Response, Electronic Discovery and Digital Investigations.

Since January 2014 she has been dedicated to defining the Global Cyber Threat Intelligence capability and is now responsible for Data Protection Services, managing the global Data Loss Prevention and Insider Threat Programs.

Bruce Churchill, InfraGard National members Alliance

Pacific Regional Representative & National Transportation Sector Chief

Bruce is a 7-year Past President of the *InfraGard San Diego Members Alliance*, serving in that capacity from 2007 to 2014. He is currently the Pacific Region Representative and the National Transportation Sector Chief for the *InfraGard National Members Alliance.*

Bruce is also the InfraGard Critical Infrastructure Sector Chief Coordinator for the *InfraGard San Diego Members Alliance* and a contributing author for the InfraGard National Disaster Resilience Council's Second Edition of *Powering Through: Building Critical Infrastructure Resilience*.

Bruce's 25-year Navy experience included assignments as Commanding Officer of the *USS Kansas City (AOR-3)*, Executive Officer of the *USS Constellation (CV-64)* and Executive Officer and Commanding Officer of *Air Antisubmarine Squadron 33* embarked on the *USS Kitty Hawk (CV-63)*.

InfraGard Today

AUTO-ISAC
Automotive Information Sharing and Analysis Center

Auto ISAC Community Call
July 6, 2022

ISACs and InfraGard

- Corporate Members
- Single Sector
- National Footprint
- Organic Analytical Capability
- Private Sector Initiative
- Self-Funded

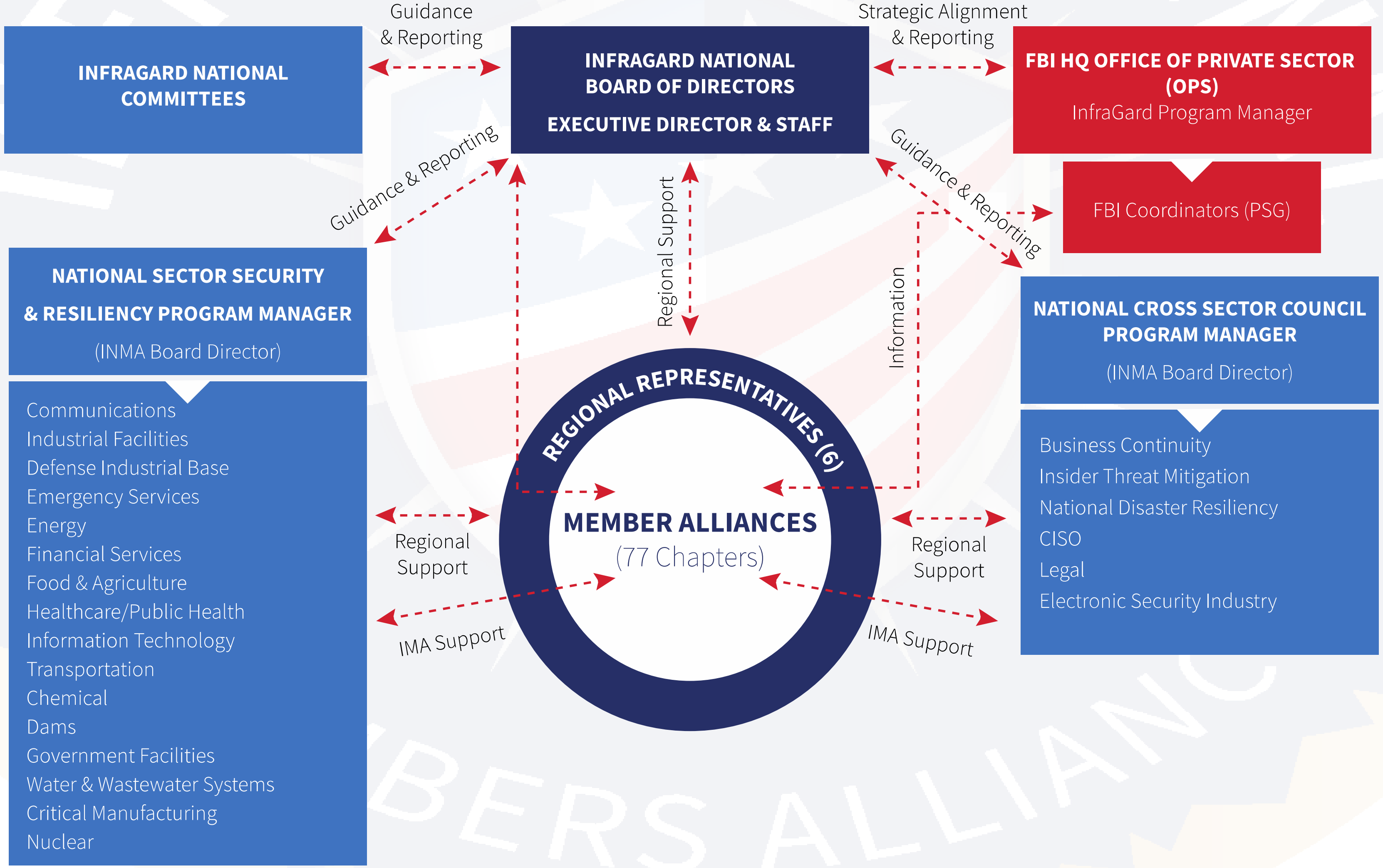
- Formal Partnership with FBI
- Individual Members vetted by FBI
- IMAs are 501(c)3 Organizations
- All Sectors (NSSRP, CSC Programs)
- Local/Regional Footprint
- No Organic Analytical Capability
- Multiple Funding Sources
  - FBI Line Item Budget (National)
  - Corporate Sponsorships
  - Grants (rare)

Why we are here ⟷

26 Years of InfraGard
1996 - 2022

- 77 Chapters/InfraGard Member Alliances (IMAs)
- **80,000+ members**
- All 16 Critical Infrastructures Sectors; both physical and cyber
- National Board of Directors – provide guidance to local chapter leadership and oversight (legal and fiscal compliance non-profit oversight)
  - FBI OPS Provides Partial Funding & ex-Officio Members
  - Certifies each local Chapter annually
- Local Board of Directors for each Chapter (all Chapters are Private Sector, Non-profit Corporations)
- FBI Private Sector Coordinator (or PSC) assigned to each Chapter acts as local FBI liaison

InfraGard National Organization



INFRAGARD NATIONAL COMMITTEES

Guidance & Reporting

INFRAGARD NATIONAL BOARD OF DIRECTORS

EXECUTIVE DIRECTOR & STAFF

Strategic Alignment & Reporting

FBI HQ OFFICE OF PRIVATE SECTOR (OPS)
InfraGard Program Manager

FBI Coordinators (PSG)

Guidance & Reporting

Regional Support

Guidance & Reporting

Information

NATIONAL SECTOR SECURITY & RESILIENCY PROGRAM MANAGER
(INMA Board Director)

- Communications
- Industrial Facilities
- Defense Industrial Base
- Emergency Services
- Energy
- Financial Services
- Food & Agriculture
- Healthcare/Public Health
- Information Technology
- Transportation
- Chemical
- Dams
- Government Facilities
- Water & Wastewater Systems
- Critical Manufacturing
- Nuclear

REGIONAL REPRESENTATIVES (6)

MEMBER ALLIANCES
(77 Chapters)

Regional Support

IMA Support

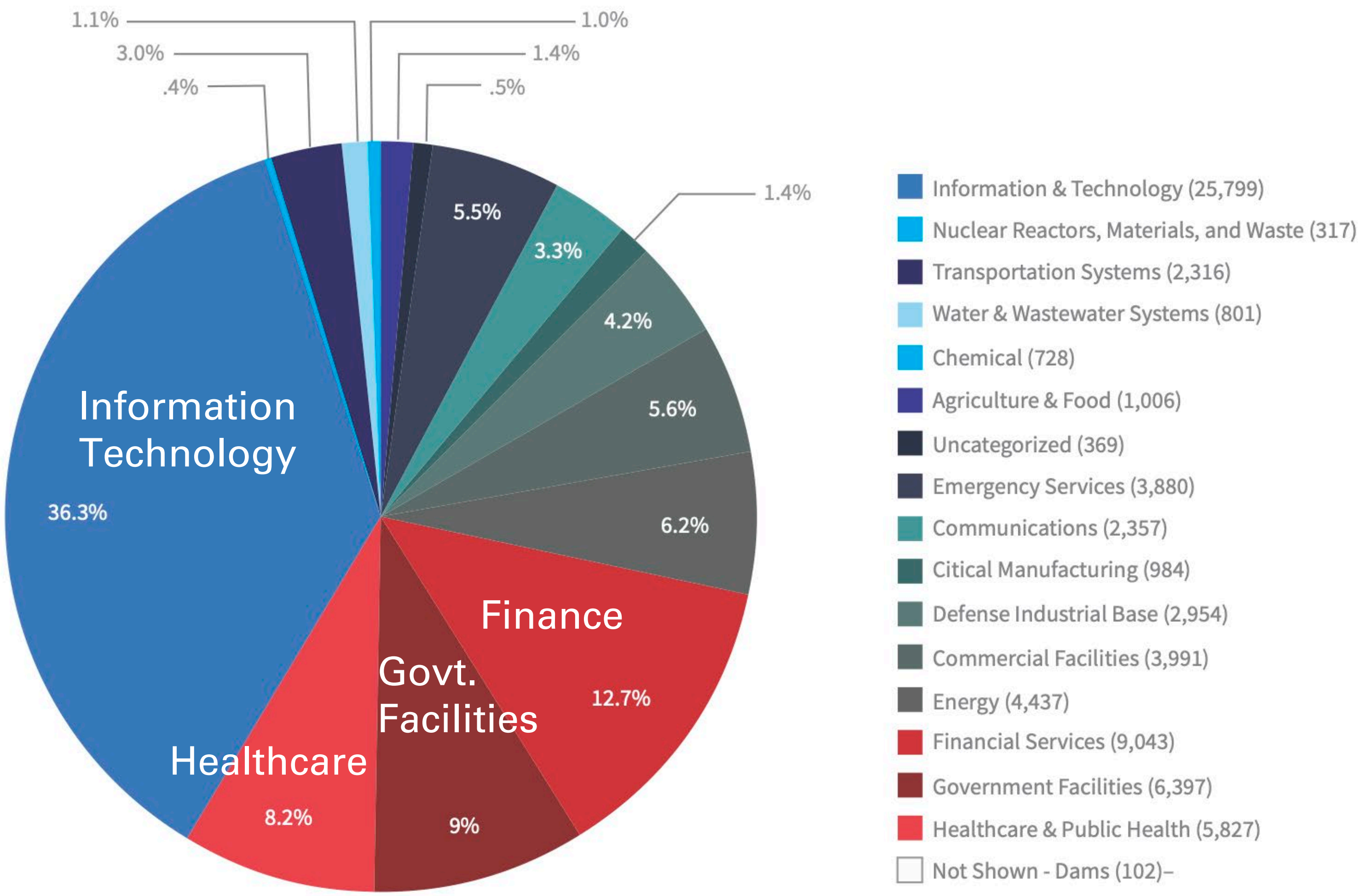
Regional Support

IMA Support

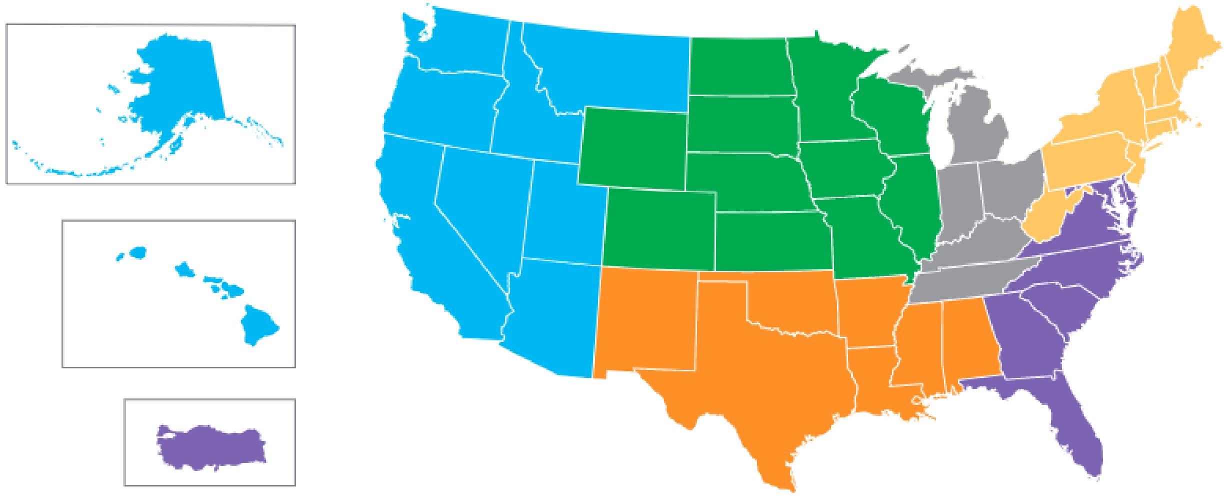
NATIONAL CROSS SECTOR COUNCIL PROGRAM MANAGER
(INMA Board Director)

- Business Continuity
- Insider Threat Mitigation
- National Disaster Resiliency
- CISO
- Legal
- Electronic Security Industry

Who are our members?

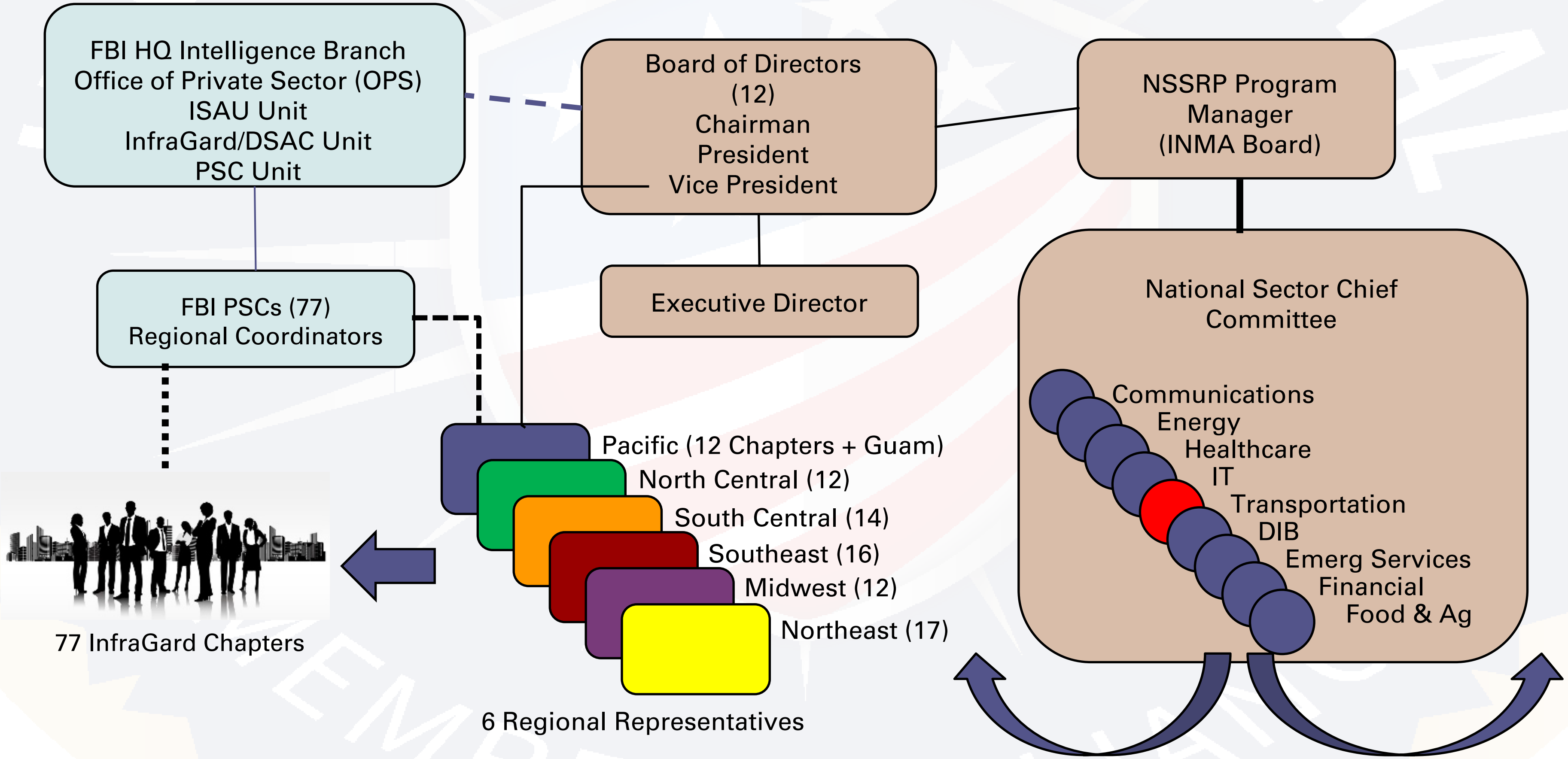


InfraGard's Six Regions



PACIFIC	MIDWEST	SOUTH CENTRAL	NORTH CENTRAL	NORTHEAST	SOUTHEAST
Alaska Honolulu Southern Nevada Sierra Nevada Los Angeles Arizona Oregon Sacramento San Diego San Francisco Bay Area Washinton State Salt Lake City Idaho	Memphis Middle TN Cincinnati Central Ohio Dayton Northern Ohio Toledo Michigan Indiana Knoxville Kentucky Southeast TN	New Mexico North Texas Mississippi El Paso Houston Arkansas Louisiana Oklahoma Mobile Austin Capital Texas San Antonio Rio Grande Birmingham Huntsville	Minnesota North Dakota South Dakota Wisconsin Nebraska Iowa Springfield Kansas City Central Missouri St. Louis Chicago Denver	Albany Vermont Boston Maine Rhode Island New Hampshire Buffalo Rochester New Jersey Connecticut NY City Metro Philadelphia Central PA Pittsburgh West Virginia	Atlanta Coastal Empire Norfolk Charlotte Eastern Carolina South Carolina Tampa Bay Orlando Jacksonville Tallahassee Maryland Delaware Nation's Capital South Florida Richmond Puerto Rico

National Sector Security & Resilience Program



FBI HQ Intelligence Branch
Office of Private Sector (OPS)
ISAU Unit
InfraGard/DSAC Unit
PSC Unit

Board of Directors
(12)
Chairman
President
Vice President

NSSRP Program
Manager
(INMA Board)

FBI PSCs (77)
Regional Coordinators

Executive Director

National Sector Chief
Committee

- Communications
- Energy
- Healthcare
- IT
- Transportation
- DIB
- Emerg Services
- Financial
- Food & Ag

- Pacific (12 Chapters + Guam)
- North Central (12)
- South Central (14)
- Southeast (16)
- Midwest (12)
- Northeast (17)

77 InfraGard Chapters

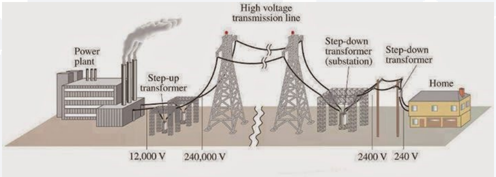
6 Regional Representatives

Sector Leadership Across 77 Chapters
Sector Partnership Building Outside
InfraGard

NDRC
National Disaster Resilience Council
A Cross-Sector Initiative of InfraGard National Members Alliance

National Disaster Resilience Council

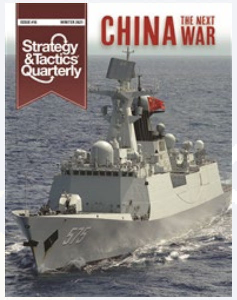
ACTIVITIES: Working Groups, Summits, Videoconferencing



Predictive Modeling – Electrical Grid

Games Simulation

Cybersecurity



36 Stratagems

Water Security

System Testing

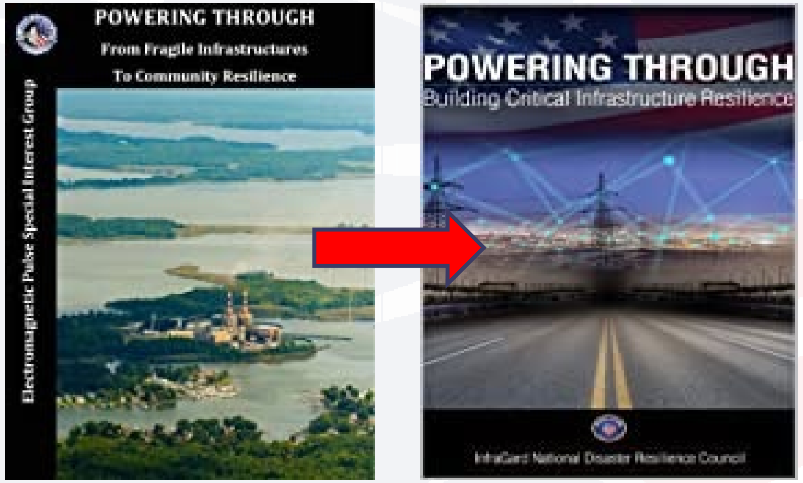
Annual Summit – Washington DC

Weekly Zoom Calls

National Disaster Resilience Council

PRODUCTS - NDRC is a recognized Thought Leader in EMP and GMD resilience

Powering Through*


POWERING THROUGH
From Fragile Infrastructures
To Community Resilience
Electromagnetic Pulse Special Interest Group
POWERING THROUGH
Building Critical Infrastructure Resilience
InfraGard National Disaster Resilience Council

2016

2021

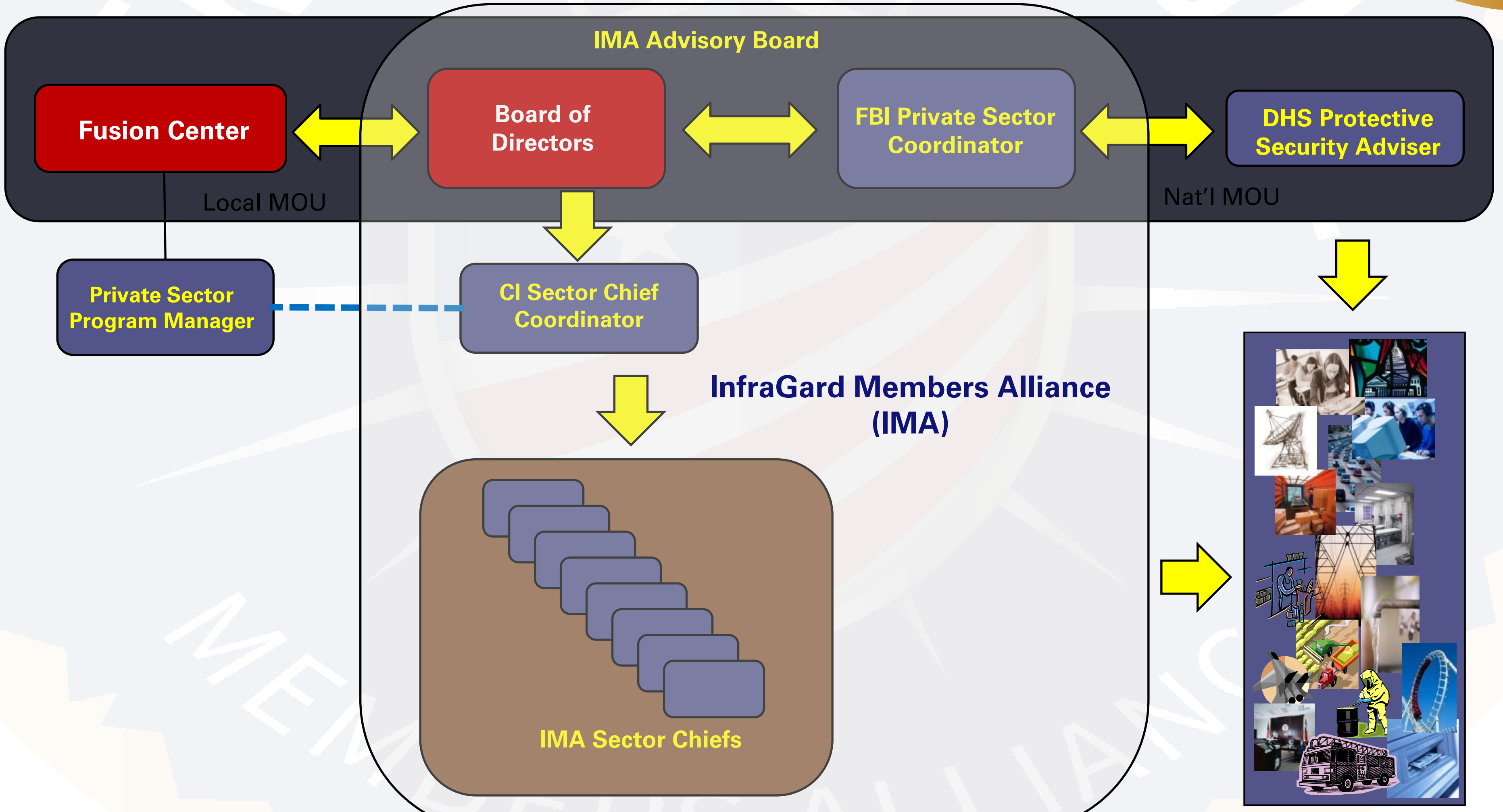
Triple Threat Power Grid Exercise Book*

2015

“*Powering Through: Building Critical Infrastructure Resilience* provides the most comprehensive review of threats, impacts, consequences, and preventative measures any organization can take to be more resilient to extended power outages that we have seen in our 16 years in the disaster management and business continuity field.”
Tom Moran, Executive Director of the All-Hazards Consortium

***Available on Amazon**

IMA-Level Sector Chief Program



IMA Advisory Board

Fusion Center

Board of Directors

FBI Private Sector Coordinator

DHS Protective Security Adviser

Local MOU

Nat'l MOU

Private Sector Program Manager

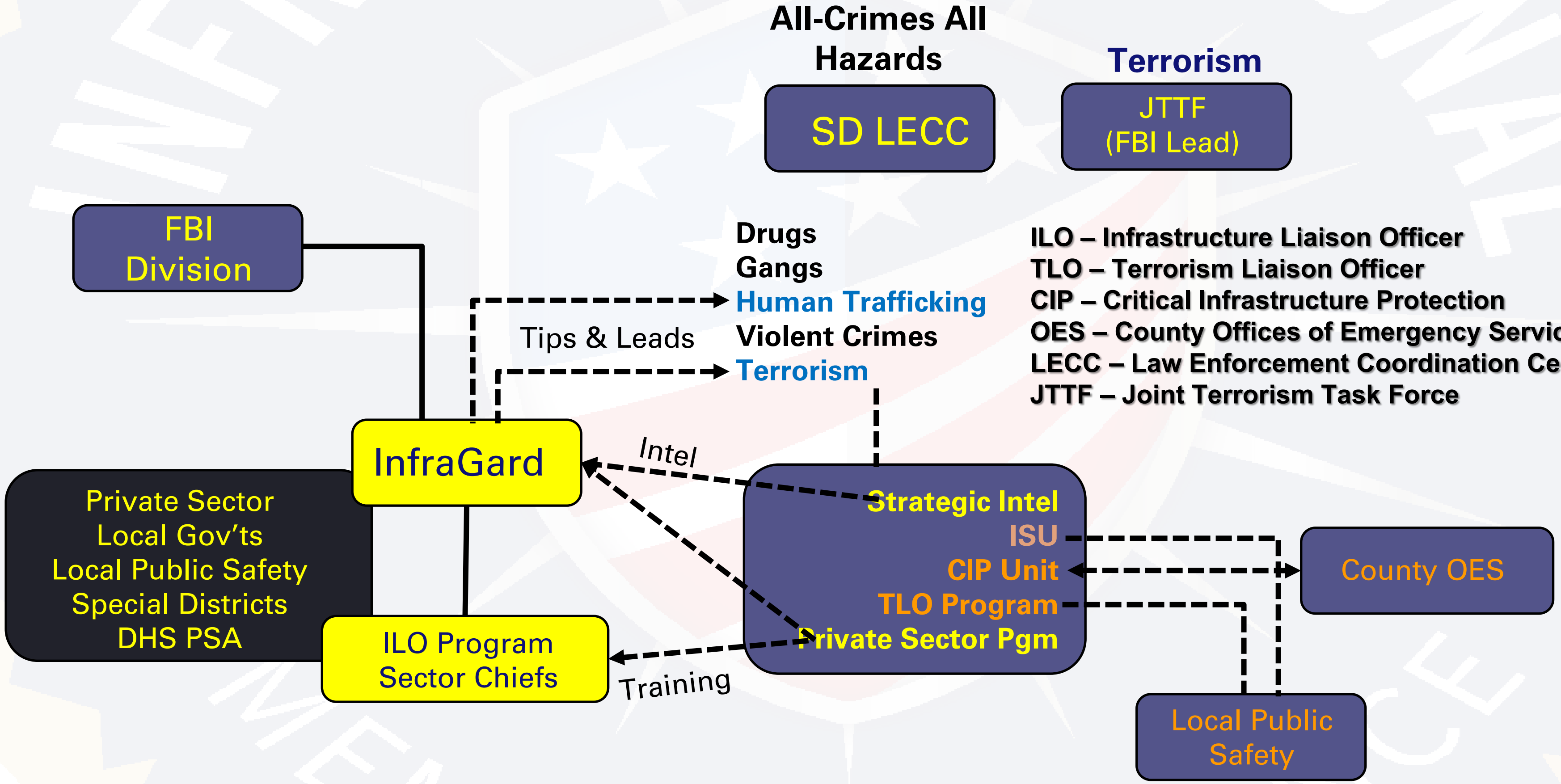
CI Sector Chief Coordinator

InfraGard Members Alliance (IMA)

IMA Sector Chiefs

Critical Infrastructure Protection

Local Partnerships - A Key to Success



All-Crimes All Hazards

SD LECC

Terrorism

JTTF (FBI Lead)

FBI Division

Drugs
Gangs
Human Trafficking
Violent Crimes
Terrorism

Tips & Leads

InfraGard

Intel

Private Sector
Local Gov'ts
Local Public Safety
Special Districts
DHS PSA

Strategic Intel
ISU
CIP Unit
TLO Program
Private Sector Pgm

County OES

ILO Program Sector Chiefs

Training

Local Public Safety

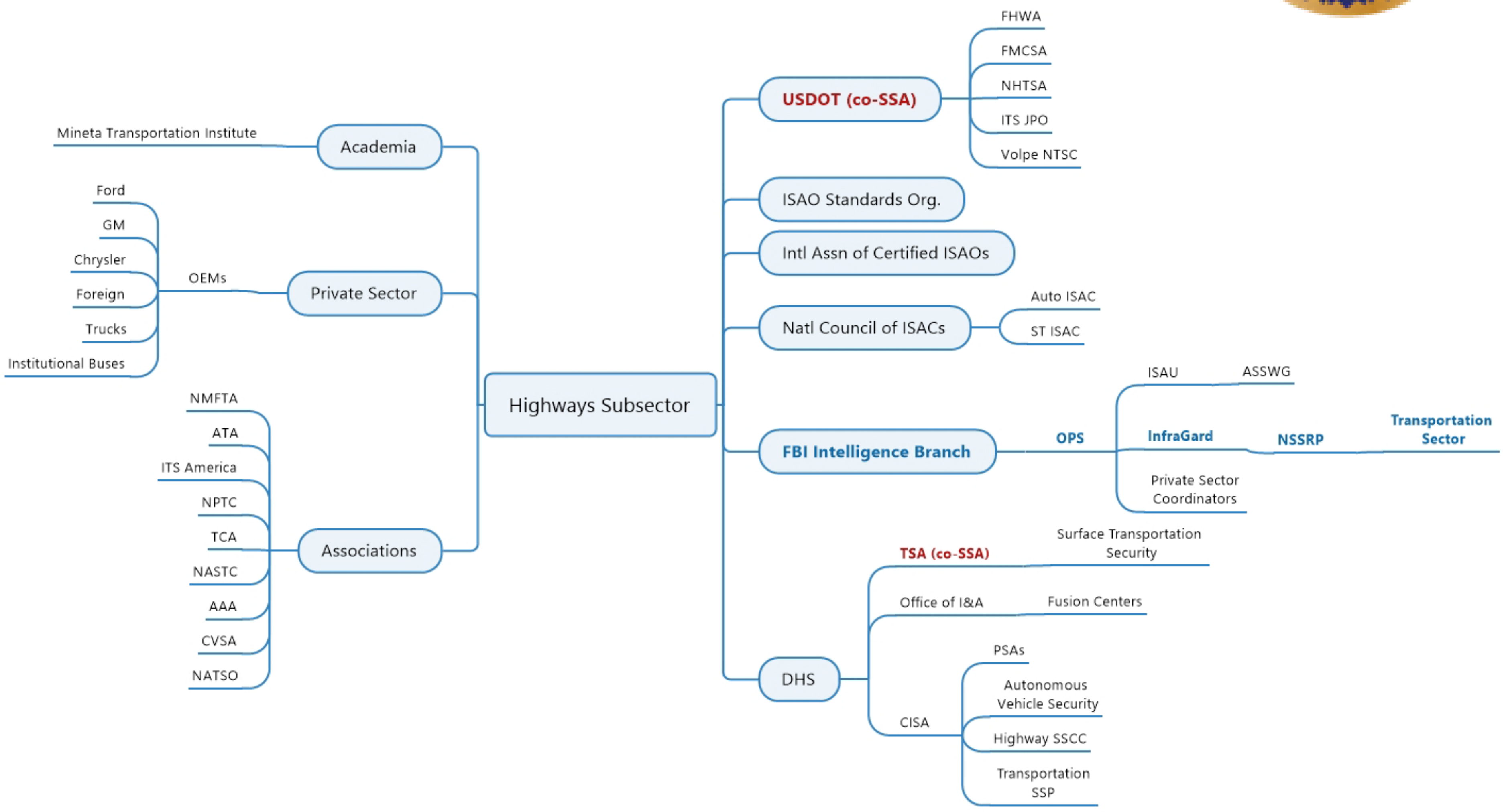
ILO – Infrastructure Liaison Officer
TLO – Terrorism Liaison Officer
CIP – Critical Infrastructure Protection
OES – County Offices of Emergency Services
LECC – Law Enforcement Coordination Center
JTTF – Joint Terrorism Task Force

InfraGard Transportation Sector

- 24 Sector Chiefs across the U.S. from San Diego to Boston and from Hawaii to Tampa Bay
  - All subsectors represented except Freight Rail
  - FBI HQ OPS ISAU
- Monthly calls led by National Transportation Sector Chief
- Scheduled Events
  - Transportation Insider Threat Webinar 2019
  - Two Unmanned Aerial Vehicle Webinars 2019
  - 2-Day Maritime Cyber Security Symposium 2021
  - Planned Supply Chain Resilience Symposium (late 2022 or early 2023)

HIGHWAY Subsector

Stakeholders – Government & Private Sector



- Highways Subsector
  - Academia
    - Mineta Transportation Institute
  - Private Sector
    - OEMs
      - Ford
      - GM
      - Chrysler
      - Foreign
      - Trucks
      - Institutional Buses
  - Associations
    - NMFTA
    - ATA
    - ITS America
    - NPTC
    - TCA
    - NASTC
    - AAA
    - CVSA
    - NATSO
  - **USDOT (co-SSA)**
    - FHWA
    - FMCSA
    - NHTSA
    - ITS JPO
    - Volpe NTSC
  - ISAO Standards Org.
  - Intl Assn of Certified ISAOs
  - Natl Council of ISACs
    - Auto ISAC
    - ST ISAC
  - **FBI Intelligence Branch**
    - **OPS**
      - ISAU
        - ASSWG
      - **InfraGard**
        - **NSSRP**
          - **Transportation Sector**
      - Private Sector Coordinators
  - DHS
    - **TSA (co-SSA)**
      - Surface Transportation Security
    - Office of I&A
      - Fusion Centers
    - CISA
      - PSAs
      - Autonomous Vehicle Security
      - Highway SSCC
      - Transportation SSP

FBI Automotive Sector Specific Working Group (Auto SSWG)

INFRAGARD NATIONAL MEMBERS ALLIANCE

The Auto SSWG is an ongoing, collaborative partnership between the FBI and U.S.-based Private Sector, which is led by the FBI Office of Private Sector's Information Sharing and Analysis Unit (ISAU)

- Electric Vehicle and Electric Vehicle Supporting Equipment
- Vehicle and fleet telematics security and infotainment systems
- Data privacy, security, and how automotive data is used in modern investigations
- Intellectual property theft in the automotive industry
- Theft activities and other criminal exploitation of vehicles
- Hosted electric vehicle webinar on 18 April for over 800 participants

AUTO-ISAC
Automotive Information Sharing and Analysis Center

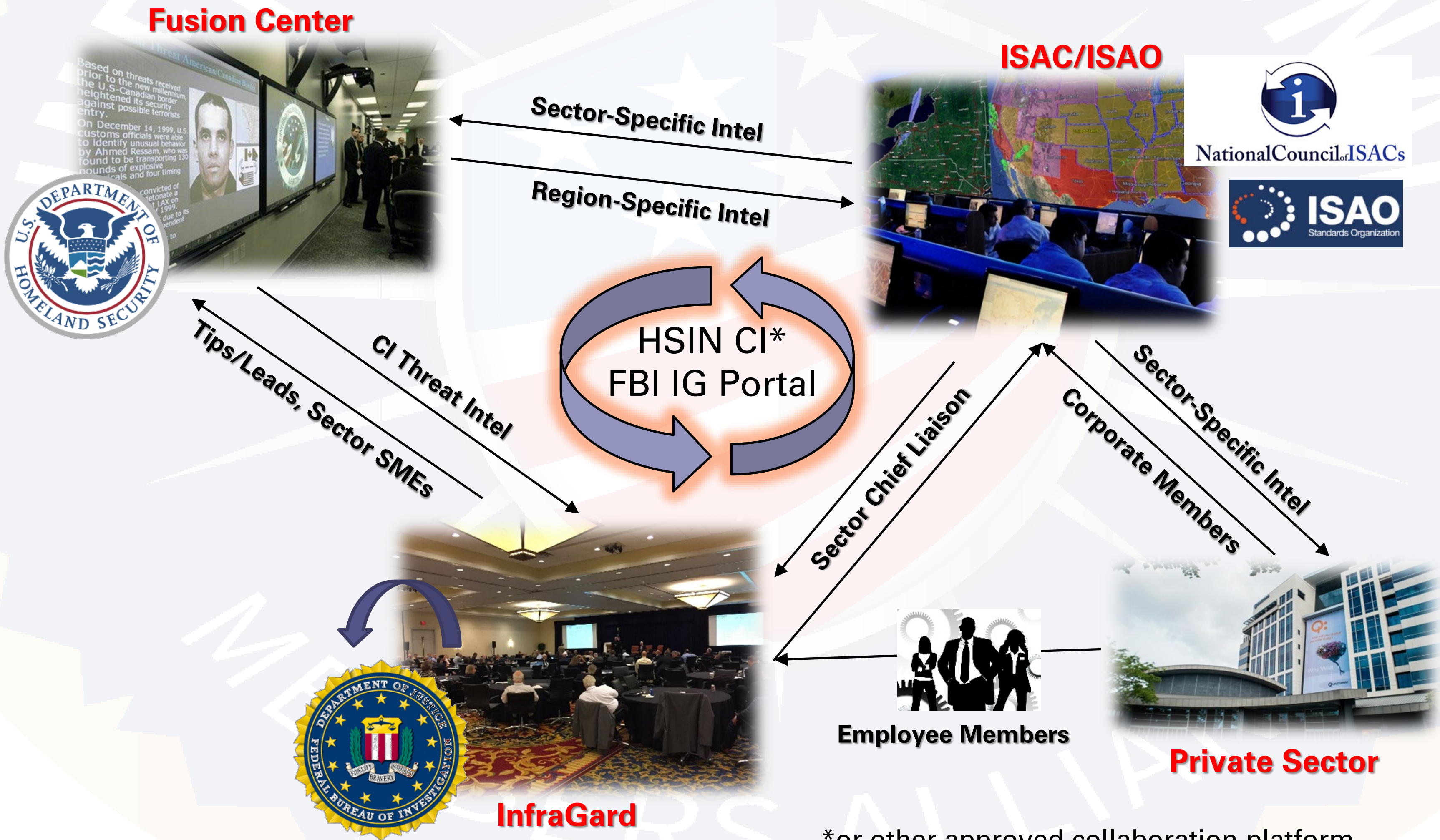
DOMESTIC SECURITY DSAC ALLIANCE COUNCIL

INFRAGARD PARTNERSHIP FOR PROTECTION

DEPARTMENT OF JUSTICE FEDERAL BUREAU OF INVESTIGATION

FEDERAL BUREAU OF INVESTIGATION OPS OFFICE OF PRIVATE SECTOR

ISAC-Fusion Center-InfraGard Collaboration Model



*or other approved collaboration platform

Questions?

Bruce Churchill
InfraGard National Transportation Sector Chief
Cell: (760) 803-2181
E-Mail: brucechurchill61@gmail.com
bchurchill@infragardnational.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, please contact andreaschunn@automotiveisac.com.
For Partnership, please contact sharmilakhadka@automotiveisac.com.

Auto-ISAC Partnership Programs

Strategic Partnership

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

1. **Must be approved** by Executive Director and the Membership & Benefit Standing Committee (MBSC).
2. Formal agreements: **NDA, SPA, SoW, CoC** required.
3. **In-kind contributions** allowed. Currently no fee.
4. **Does not** overtly sell or promote product or service.
5. Commits to **support the Auto-ISAC’s mission.**
6. Engages with the automotive ecosystem, **supporting & educating Auto-ISAC Members and its Community.**
7. **Develops value added Partnership Projects** to engage with the Auto-ISAC, its Member, and Community.
8. **Summit Sponsorship** allowed for promotion. Summit Booth **priority**.
9. Engagement **must provide Member awareness, education, training, and information sharing**
10. **Builds relationships, shares, and participates** in information sharing Auto-ISAC activities.
11. Supports our mission through **educational webinars and sharing of information.**

Community Partnership

- **Community Partners** are companies, individuals, or organizations with a complementary mission to the Auto-ISAC, with the interest in engaging with the automotive ecosystem, supporting, and educating Members and the community.
- Includes ***Industry Associations, Government Partners, Academia, Research Institution, Standards Organizations, Non- Profit, Technical Experts, Auto-ISAC Sponsors.***
- **Examples:** *Autos Innovate, ATA, ACEA, JAMA, MEMA,CLEPA, CISA, DHS, FBI, NHTSA, NCI, UDM etc.*

1. **No formal agreement** required.
2. **No approval** required.
3. Added to **Auto-ISAC Community Distro** List to stay engaged in Community events and activities.
4. Participate in **Auto-ISAC Monthly Community Calls.**
5. Learn **what is trending** in the ISACs and hear from key leaders during the **special topic of interest** presentation.
6. Added to **Auto-ISAC DRIVEN** list to receive our **daily cyber automotive newsletter.**
7. Part of the Network with **Automotive Community and the extended automotive ecosystem.**
8. Invitation to **attend and support** our yearly Summit.

Current Partnerships

Many organizations engaging

Thanks for your Support to our Many Partners

Community Partners

INNOVATOR

Strategic Partnership (17)

ArmorText

Cybellum

Deloitte

FEV

GRIMM

HackerOne

Irdeto

Itemis

Karamba Security

KELA

Pen Testing Partners

Red Balloon Security

Regulus Cyber

Saferide

Security Scorecard

Trustonic

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

2021 Summit Sponsors-

Celerium

Cyware

Denso

NDIAS

IOActive

Claroty

Deloitte

Finite State

Tanium

Recorded Future

PaloAlto Networks

Upstream

Securonix

Zimperium

Micron

Block Harbor

SecurityScorecard

Booz Allen

CybelAngel

ATT

Ford

Cybellum

2020 Summit Sponsors-

Claroty

Upstream

Escrypt

Blackberry

Cybellum

Blockharbor

C2A

Synopsis

Intsignts

ValiMail

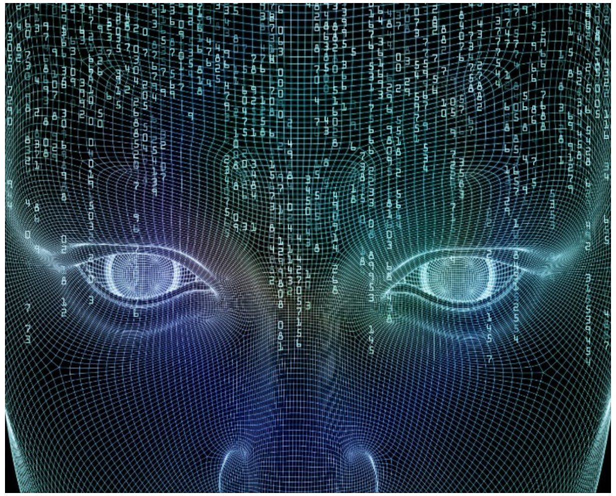
AUTO-ISAC

Automotive Information Sharing and Analysis Center

TLP:WHITE

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

Our Contact Info

Faye Francy
Executive Director

AUTO-ISAC
Automotive Information Sharing and Analysis Center

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

Sharmila Khadka
Information Technology Executive Coordinator

AUTO-ISAC
Automotive Information Sharing and Analysis Center

20 F Street NW, Suite 700
Washington, DC 20001
443-962-5663
sharmilakhadka@automotiveisac.com

AUTO-ISAC
Automotive Information Sharing and Analysis Center

www.automotiveisac.com
@auto-ISAC