



WELCOME TO AUTO-ISAC!

MONTHLY VIRTUAL COMMUNITY CALL






February 1, 2023

This Session will be recorded.

TLP: CLEAR



DHS TRAFFIC LIGHT PROTOCOL (TLP) 2.0 CHART

COLOR	WHEN SHOULD IT BE USED?	HOW MAY IT BE SHARED?
<p>TLP:RED</p>  <p>Not for disclosure, restricted to participants only.</p>	<p>Sources may use TLP:RED when information cannot be effectively acted upon without significant risk for the privacy, reputation, or operations of the organizations involved. For the eyes and ears of individual recipients only, no further.</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>TLP:AMBER+STRICT</p>  <p>Limited disclosure, restricted to participants' and its organization.</p>	<p>Sources may use TLP:AMBER+STRICT when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organization.</p>	<p>Recipients may share TLP:AMBER+STRICT information only with members of their own organization on a need-to-know basis to protect their organization and prevent further harm.</p>
<p>TLP:AMBER</p>  <p>Limited disclosure, restricted to participants' organization and its clients.</p>	<p>Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved. Note that TLP:AMBER+STRICT should be used to restrict sharing to the recipient organization only.</p>	<p>Recipients may share TLP:AMBER information with members of their own organization and its clients on a need-to-know basis to protect their organization and its clients and prevent further harm.</p>
<p>TLP:GREEN</p>  <p>Limited disclosure, restricted to the community.</p>	<p>Sources may use TLP:GREEN when information is useful to increase awareness within their wider community.</p>	<p>Recipients may share TLP:GREEN information with peers and partner organizations within their community, but not via publicly accessible channels. Unless otherwise specified, TLP:GREEN information may not be shared outside of the cybersecurity or cyber defense community.</p>
<p>TLP:CLEAR</p>  <p>Disclosure is not limited.</p>	<p>Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.</p>	<p>Recipients may share this information without restriction. Information is subject to standard copyright rules.</p>

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 Activities➤ Heard Around the Community➤ Intelligence Highlights
11:15	DHS CISA Community Update <ul style="list-style-type: none">➤ Jeff Terra, Consulting Support, Joint Cyber Defense Collaborative (JCDC), Cybersecurity and Infrastructure Security Agency (CISA)
11:20	Featured Speaker: <ul style="list-style-type: none">➤ Peter Colombo, Senior Advisor, CISA; Title: : Cross-Sector Cybersecurity Performance Goals for Critical Infrastructure
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 – *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!

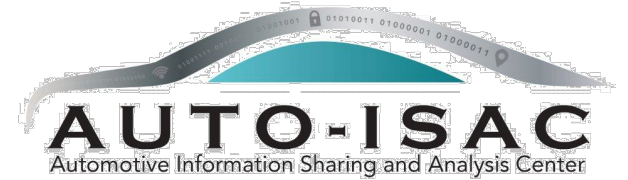
(sharmilakhadka@automotiveisac.com)



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!”*



❖ Participate

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

27
OEM Members

21
Navigator
Partners

47 Supplier &
Commercial
Vehicle 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

18
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)



TLP: CLEAR

2023 BOARD OF DIRECTORS

Thank you for your Leadership!



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



Andreas Ebert
Chair of the EuSC
Volkswagen



Larry Hilkene
Chair of the CAG
Cummins



Ravi Puvvala
Chair of the SAG
Harman



Monica Mitchell
*Member of the
Board of the Directors*
Polaris



Bob Kaster
*Member of the
Board of the Directors*
Bosch



Brian Witten
*Member of the
Board of the Directors*
Aptiv

AUTO-ISAC MEMBER ROSTER

AS OF FEBRUARY 1, 2023

Highlight = New Active Member

76 MEMBERS + 3 PENDING

Aisin	Flex	Luminar	Qualcomm
Allison Transmission	Ford	Magna	Renesas Electronics
American Axle & Manufacturing	Garrett	MARELLI	Rivian
Aptiv	General Motors (Cruise-Affiliate)	Mazda	Stellantis
AT&T	Geotab	Mercedes-Benz	Subaru
AVL List GmbH	Harman	Mitsubishi Electric	Sumitomo Electric
Blackberry Limited	Hitachi	Mitsubishi Motors	ThyssenKrupp
BMW Group	Honda	Mobis	Tokai Rika
BorgWarner	Hyundai	Motional	Toyota (Woven Planet-Affiliate)
Bosch (Ecrypt-Affiliate)	Infineon	Navistar	TuSimple
Canoo	Intel	Nexteer Automotive Corp	Valeo
ChargePoint	John Deere Electronic	Nissan	Veoneer
Continental (Argus-Affiliate)	JTEKT	Nuro	Vitesco
Cummins (Meritor-Affiliate)	Kia America, Inc.	Nuspire	Volkswagen
Cymotive	Knorr Bremse	NXP	Volvo Cars
Denso	KTM	Oshkosh Corp	Volvo Group
e:fs TechHub GmbH	Lear	PACCAR	Waymo
Faurecia	LG Electronics	Panasonic (Ficosa-Affiliate)	Yamaha Motors
Ferrari	Lucid Motors	Polaris	ZF

Pending: Bose Automotive, Fleet Defender, Micron

Upcoming Meetings:

➤ Community Call:

- Wednesday, March 1st – Time: 11 – 12:00 p.m. **TLP:GREEN**; Speaker: TBA ; Title: : TBA

➤ Members Teaching Members:

- Wednesday, February 15th – Time: 10 – 11:30 a.m. **TLP:AMBER** Rescheduled from November; Speaker: Michael Schneider, ETAS GmbH, Senior Security Consultant; Title: “Securing Modern Vehicles with AUTOSAR”

Announcements:

- ACT Program Advanced Courses – Beta Completed. Working to plan for sustainment and certification. Contact [Tamara Shoemaker](#). for more detail **(Members Only)**
- Best Practice Guide Updates – ETSC is kicking off a “Light Touch” Best Practice Guide update to bring the existing guides up to current references and standards.
- Auto-ISAC’s first European Summit will be **June 13th-14th, 2023**. More information will be available soon!
- Auto-ISAC Summit will be, **October 17th-18th, 2023** in Redondo Beach, California. Registration information and complementary passes will be coming soon.



AUTO-ISAC INTELLIGENCE HIGHLIGHT

TLP: CLEAR



AUTO-ISAC INTELLIGENCE

- Know what we track daily: [subscribe](#) to the **DRIVEN**; **TLP:GREEN** Auto-ISAC 2022 Threat Assessment is pending; Auto-ISAC Automotive Cyber Threat Ecosystem (1st Iteration) complete (TLP downgrade pending).
 - **Send feedback**, contributions, or questions to analyst@automotiveisac.com
- Intelligence Notes
 - Geopolitical tensions involving Russia, China, North Korea, and Iran remain elevated with Russia and Ukraine in crisis and Iran and Israel **near** crisis. Monitor for cyber-related spillover ([Russia-Ukraine](#), [China](#), [North Korea](#), [Iran](#)).
 - Ransomware¹ Groups Targeting Automotive: [Play](#), [Mallox](#), [BlackByte](#), [Vice Society](#), [LockBit 3.0](#) ² [Royal](#).
 - Multiple incidents of threat actors selling access to automotive organizations' networks (including VPNs) and databases. Notable Open-Source Threat Actor Forums: [BreachForums](#), [Exploit](#) and [XSS](#).
 - Notable TTPs and Tools: Endpoint Detection and Response Bypass ([DarkReading](#)); Exploitation of Control Web Panel Remote Code Execution Vulnerability ([The Hacker News](#)); Exploitation of Fortinet SSL-VPN Zero-Day Vulnerability ([Mandiant](#)); Spreading Malware via Advertisements in Google Search Results ([BleepingComputer](#)); Executing 0-day Attacks via PyPI Packages ([Fortinet](#)); [powerRAT](#) ([Phylum](#)).

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*



CISA Resource Highlights

- Joint Cyber Defense Collaborative



JOINT CYBER DEFENSE
COLLABORATIVE

Jeff Terra
2/1/2023



CISA Updates Best Practices for Mapping to MITRE ATT&CK®

- CISA updated [Best Practices for MITRE ATT&CK® Mapping](#). The MITRE ATT&CK® framework is a lens through which network defenders can analyze adversary behavior and, as CISA Executive Assistant Director Eric Goldstein noted in his [June 2021 blog post on the framework](#), it directly supports “robust, contextual bi-directional sharing of information to help strengthen the security of our systems, networks, and data.” CISA highly encourages the cybersecurity community to use the framework because it provides a common language for threat actor analysis.
- CISA coordinated this update of the best practices with the Homeland Security Systems Engineering and Development Institute™ (HSSEDI), a DHS-owned R&D center operated by MITRE. The update covers changes that the MITRE ATT&CK team made to the framework since CISA initially published the best practices in June 2021.
- The update also covers common analytical biases, mapping mistakes, and specific ATT&CK mapping guidance for industrial control systems (ICS).

• Please note all information provided is TLP Amber

NCSC-UK Releases Guidance on using MSP for Administering Cloud Services

- The United Kingdom's National Cyber Security Centre (NCSC-UK) has released a blog post, [Using MSPs to administer your cloud services](#), that provides organizations security considerations for using a third party, such as a managed service provider (MSP), to administer cloud services. Contracting with an MSP for cloud service management has become an increasingly appealing option for organizations.
 - The post discusses the trade-offs involved as well as specific security checks organizations should make to confirm the MSP's ability to defend against cyber threats.
 - CISA encourages organizations using MSPs for administering cloud services to implement the guidance NCSC-UK provides in the blog post.
- Please note all information provided is TLP Amber

CISA, NSA, and MS-ISAC Release Advisory on the Malicious Use of RMM Software

- The Cybersecurity and Infrastructure Security Agency (CISA), the National Security Agency (NSA), and the Multi-State Information Sharing and Analysis Center (MS-ISAC) released joint Cybersecurity Advisory (CSA) Protecting Against Malicious Use of Remote Monitoring and Management Software.
- The advisory describes a phishing scam in which cyber threat actors maliciously use legitimate remote monitoring and management (RMM) software to steal money from victim bank accounts.
- Criminals can sell victim account access to other cyber criminals or advanced persistent threat (APT) actors. This campaign highlights the threat of malicious cyber activity associated with legitimate RMM software: after gaining access to the target network via phishing or other techniques, malicious cyber actors are known to use legitimate RMM software as a backdoor for persistence and/or command and control (C2).
- Please note all information provided is TLP Amber

As of January 1, 2023:

- Fortinet Releases Security Updates for FortiADC
- Microsoft Releases January 2023 Security Updates
- Adobe Releases Security Updates for Multiple Products
- Drupal Releases Security Update to Address Multiple Vulnerability
- Juniper Networks Releases Updates for Multiple Products
- Mozilla Releases Security Updates for Firefox
- Apple Releases Security Updates for Multiple Products
- **Best practices:**
 - Leverage automatic updates for all operating systems and third-party software
 - Implement security configurations for all hardware and software assets
 - Remove unsupported or unauthorized hardware and software from systems

Please note all information provided is TLP Amber

- These advisories provide timely information about current security issues, vulnerabilities, and exploits surrounding ICS.
- CISA encourages users and administrators to review the newly released ICS advisories for technical details and mitigations
- Since 1/1/23 approximately 32 advisories have been issued
- The advisories span the following sectors: Information Technology, Critical Manufacturing, Energy and Multiple Sectors
- [Current Activity | CISA](#)

Please note all information provided is TLP Amber

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 added 5 new vulnerabilities to its Known Exploited Vulnerabilities (KEV) Catalog in the month of January. These types of vulnerabilities are a frequent attack vector for malicious cyber actors and pose significant risk to the federal enterprise.

Please note all information provided is TLP Amber

- ❑ CISA Homepage - [https://www\[.\]cisa\[.\]gov/](https://www[.]cisa[.]gov/)
- ❑ CISA NCAS – [https://us-cert\[.\]cisa\[.\]gov/](https://us-cert[.]cisa[.]gov/)
- ❑ CISA Shields Up - [https://www\[.\]cisa\[.\]gov/shields-up](https://www[.]cisa[.]gov/shields-up)
- ❑ Free Cybersecurity Services and Tools - [https://www\[.\]cisa\[.\]gov/free-cybersecurity-services-and-tools](https://www[.]cisa[.]gov/free-cybersecurity-services-and-tools)
- ❑ 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 Cybersecurity Directives - [https://cyber\[.\]dhs\[.\]gov/directives/](https://cyber[.]dhs[.]gov/directives/)



**JOINT CYBER DEFENSE
COLLABORATIVE**

For more information:

cisa.gov

Questions?

Central@cisa.dhs.gov

1-888-282-0870

Jeff Terra
2/1/2023





FEATURED SPEAKER

TLP: CLEAR



PETER COLOMBO, SENIOR ADVISOR, CISA

Current Positions

- Senior Advisor, Office of the Technical Director, Cybersecurity Division, CISA
- Focus are of Industrial Control Systems (ICS) and Operational Technology (OT) Strategy

Past Positions

- Program Manager, Department of Veterans Affairs
 - Managed the Department's Federally Funded Research and Development Center (FFRDC) program. A ~\$85M annual investment.
 - Component projects focused on Program Management, Systems Engineering, Acquisition Management, and Independent Verification and Validation (IV&V).
- Project Manager, Department of the Treasury
 - Led intelligence and information security projects within the Office of Intelligence and Analysis

Education

- BA – University of Virginia
- MPS – Georgetown University

CYBERSECURITY PERFORMANCE GOALS (CPGS)

DECEMBER 2022



CPGs Origin

- In July 2021, the White House issued a *National Security Memorandum (NSM) on "Improving Cybersecurity for Critical Infrastructure Control Systems."*

- Section IV of the NSM:

"[T]here is a need for baseline cybersecurity goals that are consistent across all critical infrastructure sectors."

"[C]lear guidance to owners and operators about cybersecurity practices and postures that the American people can trust and should expect for such essential services."

- Tasked CISA with three deliverables over the following 12 months:
 1. Preliminary cross-sector cybersecurity performance goals
 2. **Final cross-sector cybersecurity performance goals**
 3. Sector-specific cybersecurity performance goals (for all CI sectors)



What are the CPGs?

- What are the CPGs?

- A set of high-impact security actions for critical infrastructure organizations that address both IT and OT/ICS considerations.
- Mapped to the relevant NIST Cybersecurity Framework subcategories, as well as other frameworks (e.g., IEC 62443).

- How should organizations use the CPGs?

- Inform strategy decisions and resource investment.
- A tool to share with suppliers, vendors, and other supply chain stakeholders.

The CPG's Address:

- Account Security
- Device Security
- Data Security
- Governance and Training,
- Vulnerability Management,
- Supply Chain/Third Party,
- Response and Recovery
- Other (network segmentation, email, etc,)

CPGs At-A-Glance

CPGs Are

- A baseline set of best practices
- Intended for benchmarking operations
- For IT **and** OT owners
- Developed considering individual and aggregate risk to the nation

CPGs Are NOT

- Compulsory – CISA is not imposing requirements, but we expect the CPGs to be adopted as a standard of care
- Sector-specific
- Comprehensive/Exhaustive
- A maturity model



The CPGs and the NIST CSF

The CPGs are a voluntary tool intended to complement and not supplant or replace CSF and other commonly used frameworks and regulatory guidance!

- Should be viewed as a QuickStart guide, particularly for small and medium organizations.
- Potentially the first step on the path to full CSF alignment.
- The individual goals are mapped back to related CSF subcategories.
- The CPG CSET Module will also aid respondents in understanding which portions of CSF and MITRE ATT&CK they might be deficient in.

CPGs for Small and Medium Entities

While the CPGs are useful for any organization, they will be particularly valuable for critical infrastructure entities with a small, non-expert cybersecurity program and staff to help answer questions such as:

How do we get started?

How do we secure both OT and IT?

Which controls should we prioritize?

How do we know when we have effectively implemented these controls?

How do we show our C-Suite where investment will be most impactful?



Where to Find Them

- The most current version of the CPGs is located at [Cross-Sector Cybersecurity Performance Goals | CISA](#)
- Here you can find:



The core list of CPGs



CPG Checklist



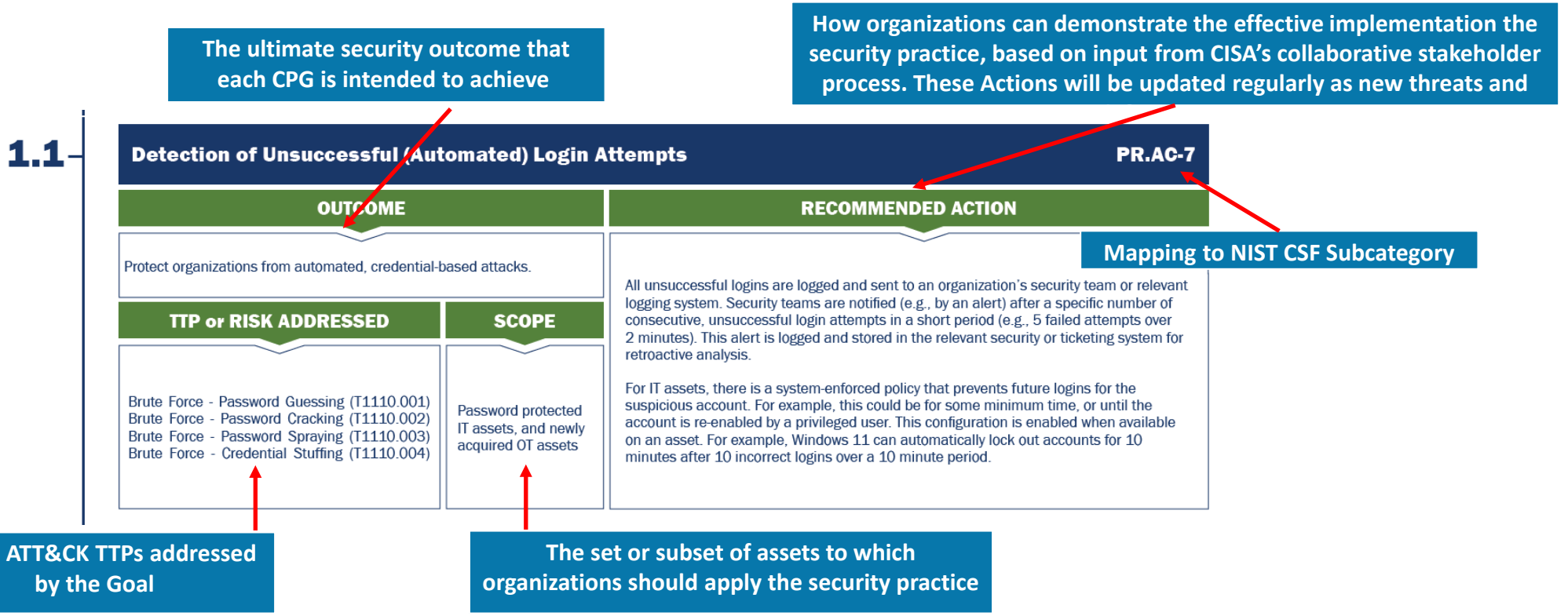
Spreadsheet of all text content



Link to our GitHub discussion page



CPGs At-a-Glance



CPG Worksheet At-a-Glance cont.

Approximate Cost/Impact/Complexity ratings to inform investment planning.

Mapping to NIST CSF

8.1 Network Segmentation PR.AC-5, PR.LPT-4, DE.CM-1	CURRENT ASSESSMENT	YEAR 1 ASSESSMENT	NOTES
<p>COST: \$\$\$\$ IMPACT: HIGH COMPLEXITY: HIGH</p> <p>TTP OR RISK ADDRESSED: Network Service Discovery (T1046) Trusted Relationship (T1199) Network Connection Enumeration (ICS T0840) Network Sniffing (T1040, ICS T0842)</p> <p>RECOMMENDED ACTION: All connections to the OT network are denied by default unless explicitly allowed (e.g. by IP address and port) for specific system functionality. Necessary communications paths between the IT and OT networks must pass through an intermediary, such as a properly configured firewall, bastion host, "jump box," or a demilitarized zone (DMZ), which is closely monitored, captures network logs, and only allows connections from approved assets.</p>	<p>DATE: <input type="text"/></p> <p><input type="checkbox"/> IMPLEMENTED</p> <p><input type="checkbox"/> IN PROGRESS</p> <p><input type="checkbox"/> SCOPED</p> <p><input type="checkbox"/> NOT STARTED</p>	<p>DATE: <input type="text"/></p> <p><input type="checkbox"/> IMPLEMENTED</p> <p><input type="checkbox"/> IN PROGRESS</p> <p><input type="checkbox"/> SCOPED</p> <p><input type="checkbox"/> NOT STARTED</p>	

MITRE ATT&CK TTPs addressed by the Goal

How organizations can demonstrate the effective implementation the security practice, based on input from CISA's collaborative stakeholder process. These Actions will be updated regularly as new threats and defenses arise.

Applicability to the Automotive Sector

Supply Chain Risk Management

- The CPGs may be valuable as a tool to either assess risk across the supply chain or vendor landscape, as well as serve as a resource to provide vendors to help them raise their cyber maturity level.

As a tool for understanding applicability and overlap of various regulatory frameworks

- CISA has heard from many owners/operators of CI regarding the challenges of understanding how to apply cybersecurity guidance across sectors or varying regulatory environments (e.g. international). The CPGs, through being mapped to various sector guidance, may aid in understanding how adherence to one framework may translate to applicability to others.



Development Process

During both the development and the continued management of the CPGs, CISA is committed to ensuring that they are the product of collaborative engagement with the stakeholder community.

- The first draft of the performance goals was published September 2021, garnering nearly 1,000 comments.
- The team consulted and received feedback from experts across the cybersecurity community, including the inter-agency, critical infrastructure organizations, individual experts, and international partners
- As part of the second feedback round in the Summer of 2022, CISA conducted multiple workshops and listening sessions, and received an additional 700+ comments.
- Key Themes from the feedback process included:
 - Closer Alignment to the NIST Cybersecurity Framework
 - Prioritization of Goals – which are most important to implement
 - Outcome Oriented Vs. Prescriptive Goals
 - Concise Scope - clearly delineate applicable assets
 - Language – removal of absolute terms (all/must)



Upcoming Changes

v1.0.1

- CISA will be publishing a minor update in mid/late February. Edits will include:
 - Rewording of MFA Goal to align with recent CISA guidance.
 - A new goal focused on recovery.
 - Recategorization and reordering of the existing goals to align to the NIST CSF functions.



Catalyzing Adoption

Rollout

- CPGs were formally launched on October 25, 2022!

Adoption

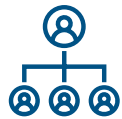
- Incorporating the CPGs into CISA's guidance and services to help enable adoption and measurement.
- Conduct focused outreach to Sector Risk Management Agencies to enable sectoral adoption
- Posting on CISA.gov and Github with open request for feedback



Future Updates



- CISA will continue to manage and update the CPGs on a recurring cadence
- Utilizing GitHub and other methods to develop a backlog of future changes and updates.



Management Structure

- CSD leadership is currently analyzing approaches for where and how to continue to manage the CPGs as a flagship CISA product.
- One of the most likely approaches is to establish a PMO that will be responsible for outreach and training, solicitation of feedback, and drafting of future iterations.



Sector-Specific Goals

- Development will be SRMA led, with CISA responsible for ensuring a level of commonality and structure (e.g., groupings, taxonomy).
- The specificity will likely be determined by the average maturity level of a given sector and the unique requirements of their component subsectors.
- Will likely be executed in a series of flights of approximately 4 sectors each. (18-24 month effort).
- The initial flight to be addressed will include **Energy, Chemical, Financial Services, and IT** sectors.





For more information:
Cybersecurity Division
Office of the Technical Director
Daniel.Bardenstein@CISA.DHS.gov
Peter.Colombo@CISA.DHS.gov

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 melissacromack@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
(18)**

ArmorText
 Cybellum
 Deloitte
 FEV
 GRIMM
 HackerOne
 Irdeto
 Itemis
 Karamba Security
 KELA
 Pen Testing Partners
 Red Balloon Security
 Regulus Cyber
 Saferide
 Security Scorecard
 Trustonic
 Upstream
 Vultara

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
 OASIS
 ODNI
 Ohio Turnpike & Infrastructure Commission
 SANS
 The University of Warwick
 TSA
 University of Tulsa
 USSC
 VOLPE
 W3C/MIT
 Walsh College

BENEFACTOR

**Sponsorship
Partnership**

2022 Summit Sponsors-
 Argus
 BGNetworks
 Bosch
 Blackberry
 Block Harbor
 BlueVoyant
 Booz Allen Hamilton
 C2A
 Cybellum
 CyberGRX
 Cyware
 Deloitte
 Denso
 Finite State
 Fortress
 Itemis
 Keysight Technologies
 Micron
 NXP
 Okta
 Sandia
 Securonix
 Tanium
 UL
 Upstream
 VicOne

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!



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
[@auto-ISAC](#)



TLP: CLEAR