Governmental Committee

November 1, 2016

Las Vegas

COMMITTEE MEMBERS

STEPHEN REGAN, CHAIR
JANET CHANEY, VICE-CHAIR
DAVE McCLUNE
HERB LIEBERMANN
RANDY HANSON
HOWARD BATCHELOR
JEANNIE SILVER
RICK TUURI
RON REICHEN
STEVE DANIELS
TIM ADELMANN
BOB SMITH
DARRELL AMBERSON

- Regan Strategies
- Cave Creek Business Development
- California Autobody Association
- LKQ Corp
- Allstate Insurance Company
- Georgia Collision Industry Assoc.
- CARSTAR, Mundelein
- AudaExplore, a Solera Company
- Precision Body and Paint
- LaMettry's Collision
- Capitol Collision
- GMG EnviroSafe
- LaMettry's Collision

ASA Washington, D.C. Office
Robert Redding

CIC | November 1, 2016

Telematics update

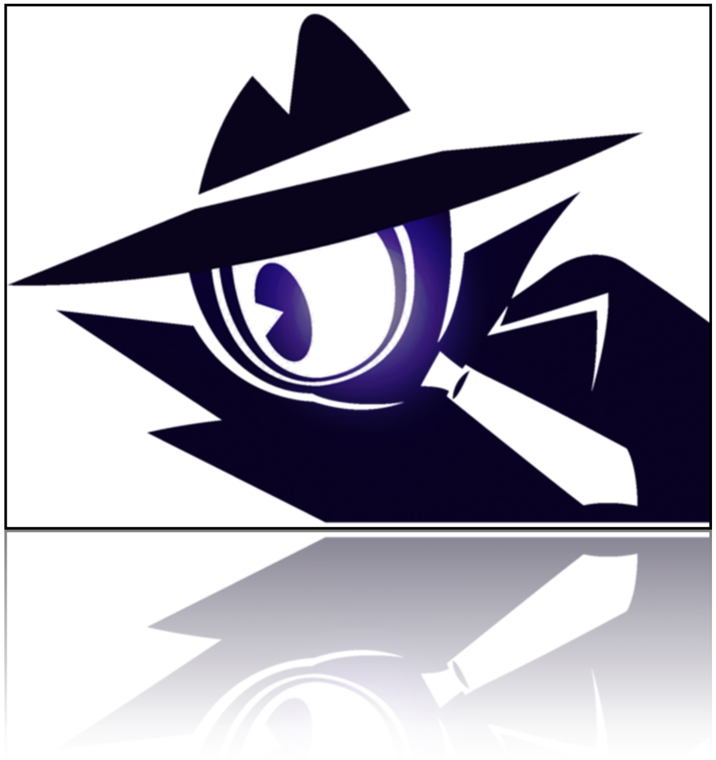
- **July 2014: ASA and the Alliance of Automobile Manufacturers hold the first Technology and Telematics Forum (TTF) at NACE|CARS with 250 registered participants.**
- **February 2015: ASA hosts OEM/aftermarket roundtable in Dallas, Texas, with 32 automotive organizations represented.**
- **July 2015: ASA hosts policy discussion with aftermarket leaders and key OEM representatives.**
  - ASA and the Alliance host the second TTF program at NACE|CARS.

Telematics update

- **July 2016: ASA co-hosts telematics update webinar with the Alliance and MEMA.**
- **August 2016: ASA and the Alliance host third TTF program.**
- Aftermarket Telematics Taskforce-OEM Status Report

Cyber Security

- How does cyber security relate to telematics and new technology strategy for the aftermarket?
- For Automakers?
- Federal Legislation
- State Legislation



NHTSA Cybersecurity Best Practices for Modern Vehicles

- On October 24, 2016, NHTSA issued its proposed guidance for improving motor vehicle cybersecurity.

- The guidance recommends:

  - risk-based prioritized identification and protection of critical vehicle controls and consumers' personal data;
  - making cybersecurity a top leadership priority for the automotive industry;
  - best practices for researching, investigating, testing and validating cybersecurity measures.

Auto Information Sharing and Analysis Center

- NHTSA encouraged the industry to create the Auto-ISAC and invite all stake holders to participate.
- Jan 2016 the Auto-ISAC began
- ISAC is an information sharing and analysis center initiative.
- Much of it is anonymous to allow competitors to share problems they have discovered.

AUTOMOTIVE INFORMATION SHARING AND ANALYSIS CENTER

An industry-operated environment created to enhance cyber security awareness and coordination across the global automotive industry

Auto Information Sharing and Analysis Center

- Other industries such as Air Travel have ISACs
- The auto industry is the first to create an ISAC before a major accident occurred.
- Primarily focused on vehicle and data security

AUTOMOTIVE INFORMATION SHARING AND ANALYSIS CENTER

An industry-operated environment created to enhance cyber security awareness and coordination across the global automotive industry

Federal Legislation - 114th Congress

□ US H 2886, Rep. Dan Lipinski (D-IL)- Automated and Connected Vehicle Research Initiative

□ US H 3876, Rep. Grace Meng (D-NY)- Autonomous Vehicle Privacy Protection Act

□ US H 3994, Rep. Joe Wilson (R-SC)- Appropriate Cybersecurity Standards for Motor Vehicles

□ US S 1806, Sen. Ed Markey (D-MA)- Motor Vehicle Security and Privacy Threats

State Legislation

- CA A 1592- Autonomous Vehicles: Pilot Project (enacted)

- MA HB 4321- Operation of Autonomous Vehicles Without Active Control (pending)

- MO SB 923- Connected Vehicle Technology Testing Program (adjourned)

- OH HB 608- Authorizes Autonomous Vehicles to Operate on Public Roads and Highways (pending)

- RI SB 2514- Allows Vehicles Equipped with

NHTSA’s Federal Automated Vehicles Policy

- On September 20, 2016, NHTSA issued its policy for automated vehicles, opening a route to the testing and deployment of new auto technologies.

- The policy consists of four key parts:

  - 15-point Safety Assessment
  - Model State Policy
  - NHTSA’s Current Regulatory Tools
  - Modern/Future Regulatory Tools

NHTSA Cybersecurity Best Practices for Modern Vehicles

- **There are a couple of key topics of interest to repairers that have been addressed with recommendations by NHTSA**
- **Security of vehicle owner private data**
- **Diagnostic Tool Recommendations**
  - **Workshop environment threat vectors**
  - **Identification of Devices to consider**

6.7.3 Control Vehicle Maintenance Diagnostic Access

Diagnostic features should be limited as much as possible to a specific mode of vehicle operation which accomplishes the intended purpose of the associated feature. *Diagnostic operations should be designed to eliminate or minimize potentially dangerous ramifications if they are misused or abused outside of their intended purposes.* For example, *a diagnostic operation which may disable a vehicle’s individual brakes could be restricted to operate only at low speeds*. In addition, this diagnostic operation might not disable all brakes at the same time, *and/or it might limit the duration of such diagnostic control action.*

6.7.3 Control Vehicle Maintenance Diagnostic Access

What does this mean for repairers?

- **As we have in the past with items like OBD II and Mode $06 diagnostic information for example, repairers must partner with OEs and scan tool makers to ensure that tests are useful to our diagnostic and repair processes.**
- **This also means that as the automotive industry evolves processes, repairers need to be proactive and patient in helping to protect drivers from cyber threats.**
- **Our own ability to repair vehicles may depend on it.**

What should I do as a repairer?

- Adopt best practices in your business for cyber security.
- Place all internet connected tools and workshop use devices on a closed/isolated Scan tool network with a firewall
- Consider shop policy prohibiting taking scan tools home or connecting tools or personal computers including tablets and phones into the “Scan tool network”
- ASA is developing a training program for service technicians to teach them cyber security best practices and how to control basic wired and wireless security in the shop.

Tools to Consider Securing

- Scan Tools
- Alignment Machines
- Digital cameras with internet connections
- Service information PCs or Tablets
- An IT professional can configure a stand-alone wireless SSID for this equipment
- Making the SSID hidden will not enhance security from professional hackers

Type of Connections to Secure

- Wireless Networks
- Wired Networks
- Bluetooth devices or tools – especially long range devices

Driver Personal Data

- **NHTSA sites several sources from FTC, NIST and others to define "Personally Identifiable Information" PII**
- **Generally accepted PII definition is:** "any information about an individual, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information." – NIST (national institute for standards and technology)

Driver Personal Data

- Vehicles can or will be able to track new data that includes
- Location, speed, direction
- Credit Card information to complete on-the-road purchases
- Biometrics to determine driver attentiveness

Driver Personal Data

- Imagine if a bluetooth device installed for insurance or some other use were delivering that data without driver or the bluetooth device's creator awareness.
- It's a brave new cyber-physical world.
- Repairers need to be vigilant and help vehicle owners understand both our roles and their roles in keeping the road safe.

Thank you!

CIC