Welcome to GSA Fleet's Connected Vehicles Workshop

Audio: Everyone is automatically muted. Listen via your computer audio if possible.

Presentation & Certificate: You can download a copy of the presentation at https://www.gsa.gov/gsa-fleet-training. Additionally, a copy of the presentation along with a certificate will be emailed after the session.

Questions: Use the Q&A window to ask questions at any time. You may get a typed response or it may be answered aloud at the end of the presentation.

Recorded: The session will be recorded.
Recordings of GSA Fleet Desktop Workshops are available at: http://bit.ly/DtWRecordings

Connected Vehicles Training

GSA Fleet
Desktop Workshop
05/22/2024

Agenda

Purpose and Learning Objectives

Purpose

To provide the Federal fleet community with a foundational understanding of connected vehicles and the associated impacts that connected technology has on fleet operation and management.

This training will equip fleet operators and managers with the information, resources, and best practices needed to optimize use of connected technology and mitigate against potential risks and pitfalls.

1. **Educate**
   Understand the impacts of connected vehicles and connected technology and how emerging trends will impact the federal fleet community

2. **Act**
   Apply lessons learned to proactively manage and realize the benefits of connected vehicles and connected technology.

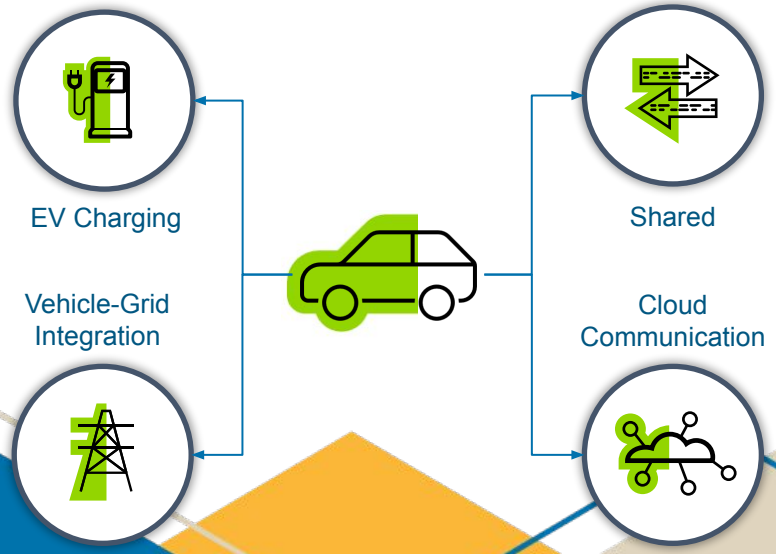
3. **Mitigate**
   Proactively protect against risks and potential pitfalls associated with connected vehicles and connected technology

4. **Share**
   Provide resources to equip federal fleet managers and operators with the information needed to sustain both short- and long-term operational continuity.

Introduction to Connected Vehicles

Overview – What is a Connected Vehicle?

- Connected Vehicles are vehicles that can communicate bidirectionally with other systems outside the vehicle
- This presentation will focus primarily on how Connected Vehicles communicate with OEMs and fleet management software, and the risks associated with new ways of operating vehicles



TAKEAWAY

Connected vehicles interact with the environment around them in ways that were not previously possible. This allows for **benefits** such as being able to **receive software updates, better understand driving patterns and routes, and utilize a variety of cutting-edge technologies**. However, this also opens the door to new **risks**, such as the **potential for data theft and/or cybersecurity intrusion into the vehicle**.

The Connected Vehicle Journey

1990s

The era of connected vehicles began with the launch of embedded telematics systems such as OnStar in the mid-1990s. These systems provided hands-free voice calling capabilities and connected vehicles to OEMs' call and data centers to provide a variety of services such as roadside assistance.

2000s

In the 2000's, vendors improved designs and commercialized their technologies, collecting large amounts of data, but also introducing new types of threats to vehicles. The mobile phone revolution and ubiquitous high speed data connectivity has transformed the way people and things communicate.

2010s

Virtually every newly built vehicle in North America—and most vehicles globally—is connected. These technology enhancements open private citizens, OEMs, and large fleet operators to vulnerabilities related to personal information, data security, and unauthorized access to vehicle information systems.

1990s | **2000s** | **2010 - Present**

1990
Mazda Eunos Cosmo is first mass-production car with GPS

1996
GM launches EV1

OnStar, the first embedded telematics and crash notification system, debuts at Chicago Auto Show

Lincoln releases Remote Emergency Satellite Cellular Unit for roadside assistance

1997
NAHSC Automated Highway Test

2005
TomTom builds fleet management platform and calculates route travel times

2006
OnStar develops turn-by-turn navigation

2007
Launch of the iPhone

Inverse Path demos hack of car's satellite navigation system

2008
Progressive offers Snapshot for usage-based insurance (UBI)

2010
A disgruntled ex-car dealership employee remotely disables >100 cars

2015
OnStar mobile app hack at DEF CON Conference

2019-2022
Tesla workers viewed and shared private videos from cars

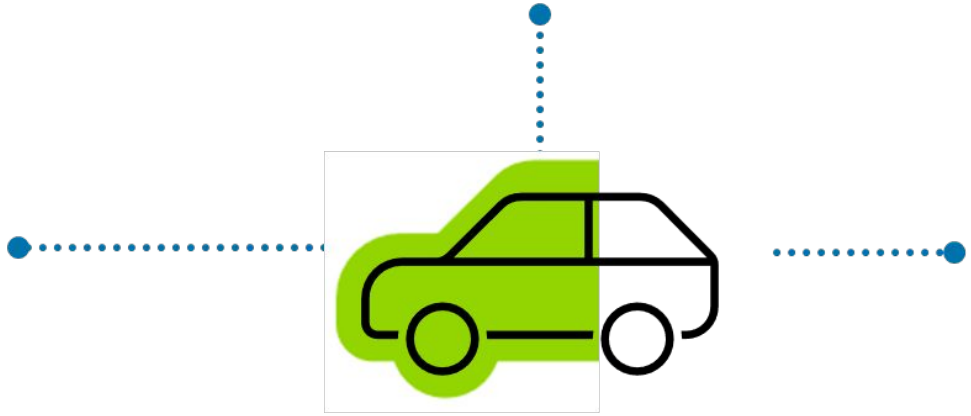
Why Are Connected Vehicles Unique?

Electric Vehicles

- EVs require connectivity
  - The way the vehicle runs can be radically changed through OTA updates because the components are connected and controlled by code
  - The ability to communicate with a charger and charging networks requires connectivity through the air and/or the charging port

Connected Vehicles

- Connected vehicles allow drivers to remotely unlock the vehicle, check location, see fuel or charge status, update infotainment, and report telematics
- OEMs have stated that all vehicles will be connected going forward
- Level of connectivity will differ depending on vehicle type



Gas/Hybrid Vehicles

- ICE vehicles require less connectivity, but are typically implemented for comfort and convenience features
  - Preconditioning cabin requires engine start
  - Same infotainment, telematics, and remote capabilities
  - Can still benefit from security and stability updates

Connected Vehicles Benefits & Risks

Benefits

Remote Updates and Recalls:

- Recalls can be addressed immediately through OTAs
- OEMs can push out optional updates to vehicles to improve performance, fix bugs, and improve security.

Vehicle Safety:

- GPS connection allows fleet managers to monitor vehicle location
- Fleet diagnostics enables remote issue diagnosis
- Software security issues remote issue resolution

Driver Monitoring:

- Unsafe driver behavior (speeding, sudden braking, etc.) can be observed by fleet manager

Risks

Vehicle Security:

- More points of entry than traditional vehicles that can be exploited by bad actors
- Vehicles track and archive driver information, including personally identifiable information

Obsolescence:

- Stranding of assets can occur due to rapid advancements in vehicle technology if fleet operators are not ready

Operational Complexity:

- New operators not used to vehicle connectivity and applications may be vulnerable to cybersecurity risks
- Connected vehicles have features and capabilities that have a learning curve for new operators

Connected Vehicle Technology

Connected Technology Overview

- Vehicles are connected through onboard computers communicating with servers through cellular and satellite connection
- Satellite connectivity allows for built in GPS navigation, advanced security features, and fleet monitoring.
  - Allows for driver behavior tracking and increased vehicle security
- Cellular connectivity allows for wireless updates and internet access
  - Firmware updates can improve hardware calibration such as battery and charge management
  - Infotainment updates can improve maps, user interface, and driving apps
- Comfort and Convenience features
  - Remote access, remote start, cell phone connection

Over-The-Air (OTA) Updates

What is an Over-The-Air Update?

OTA updates allow vehicles to receive critical information for devices and ensure proper functionality.
OTA updates are transmitted remotely from a cloud-based server through a cellular or Wifi connection to a connected vehicle. OTA updates can be installed automatically, allowing vehicles to have the latest updates as soon as they are available.

There are two types of OTA Updates, 1) Software and 2) Firmware

Software

- Software updates are pushed to vehicles more frequently than firmware updates.
- Software updates are primarily targeted at vehicle infotainment systems – they include map, audio system, interface, and feature upgrades updates to map information, supplying audio upgrades
- Software updates improve the in-car experience but do not impact the vehicle's performance.

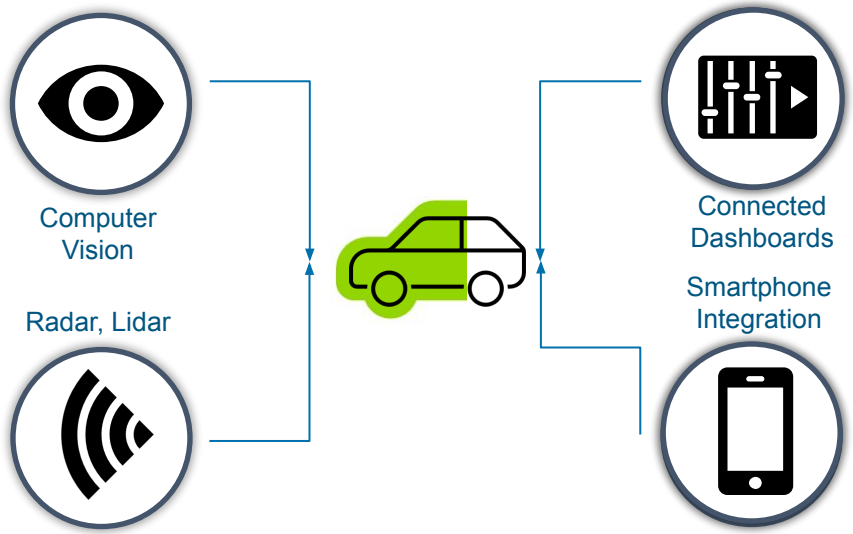
Firmware

- Firmware updates impact the vehicle's ability to safely operate.
- These updates can provide enhancements or corrections to the powertrain systems, chassis systems, and advanced driver assistance systems.
- Firmware updates allow auto manufacturers to push performance and efficiency updates based on continuously monitored real-world driving data.
- OTA update install time can range from less than 20 minutes to several hours depending on the size of the update.

Cameras, Sensors, and Infotainment

Cameras and Sensors

- Vary greatly vehicle to vehicle but will always include a backup camera and proximity sensors.
- Higher-level ADAS systems require cameras, radar, or LiDAR for their functioning
- Sensor fusion from multiple sources ensure security and reliability
- Driver monitoring sensors



Infotainment

- Infotainment systems are the bulk of the ways that a driver will interact with the vehicle
  - Controls media, navigation systems, and various parts of the driving experience
- Some OEMs (like Tesla) make their infotainment systems prominent and necessary. Some (like Volvo) ship more minimalist infotainment system options
- Certain features may expose security issues
  - Voice commands might require cloud computing for language processing, involving a connected server and additional privacy concerns

Data & Application Management

- Data includes location, routes, charging timing, battery or fuel levels, speeds, and braking or acceleration events
- Security Concerns
    - Data is typically anonymized but can still reveal information about drivers such as home or work locations.
    - OEMs retain information connected to each vehicle, such as identifiers, payment and financial information, driver behavior, and even biological characteristics
- Fleet managers can utilize Application Program Interfaces (APIs) to manage data
    - These allow users and operators to handle vehicle data to draw their own insights
    - Only certain vehicle OEMs offer APIs, so this should be checked
    - Fleet managers can utilize the vehicle data to find specifics in their fleet
        - Driver behavior, state of charge, and other diagnostics
    - They can also utilize this to push updates and recalls to vehicles in a convenient way.

Impacts to the Federal Fleet Community

Operational Impacts

Impact	Description
Increased Learning Curve	Introduction of connected vehicles into existing fleets will require targeted training and guidelines to equip drivers with understanding of operational basics.
Subscription-Based Access to Capabilities	Subscription fees for some CV features need must accounted for and may have adverse financial impacts on fleet management organizations.
Proactive Software Update Monitoring	Software-related updates will require a plan to monitor software versions and perform updates in a timely manner, both for OTA and at service facilities.
Access to Maintenance and Repair Facilities	The complexity of connected cars could mean that third-party electronic diagnostics are unavailable or prohibitively expensive, and that some service must be performed by authorized service centers such as dealerships.
Enhanced Fleet Management Capabilities	The potential to remotely track vehicle mileage and any malfunction codes will allow fleets to anticipate service needs more accurately and reduce down-time.
Proactive Risk and Performance Monitoring	Real-time monitoring, if implemented, can allow for evaluation of drivers to ensure compliance with traffic laws and encourage fuel-efficient driving behavior.

Cybersecurity Impacts

Impact	Description
Data Management and Security	Connected vehicles have the potential to transmit and receive data from multiple sources, including OEM cloud storage as well as third-party partners that OEMs and service providers work with. There is currently a lack of regulatory standards to ensure the secure custody of this data.
OEM Data Collection and Controls	Automaker terms and conditions allow for the collection of vast amounts of data collection around vehicle operation and use, and many automakers reserve the right to sell this information to third parties. This creates additional risks around privacy and security.
Added Cybersecurity Risk Through Multiple Threat Vectors	The interconnection of vehicle systems means that there are multiple attack vectors for bad actors and greater potential for vehicle operation to be impacted.
Software Security Planning and Upgrades	An action plan for software security patches is required to update vehicles systems as quickly as possible or to disable some connected features until an update can be performed.
Vehicle Hardware Considerations	This extends to the vehicle hardware, which can be used to compromise unrelated systems. Therefore, extra attention should be paid to damage or vandalism in order to ensure it is not masking an electronic attack.
Vehicle End of Life & Obsolesce	Manufacturers will end software and firmware support for each model at some future point, similar to mobile device and computer operating software. Older cars may need to be replaced to avoid potential security vulnerabilities.

Fleet Manager & Operator Best Practices

Operations Best Practices – Focus Areas

Vehicle Access & Operations

- Training for vehicle users should involve best practices on driving, charging, maintaining, and updating the vehicle
- Fleet operators can work with a 3rd party telematics company rather than the OEM if they want control over their vehicles' data
- "Fobless" entry is a developing technology. GSA will work with OEMs and will periodically put out new guidance to fleet managers regarding vehicle alternatives if the desired fleet vehicle goes "fobless"

Software Updates

- Fleet managers should stay aware of when OTA updates, which include software and firmware updates, are released
- Fleet operators should log the current version of software and firmware available, and send out periodic instructions with update procedures (including where / when the update will occur)
- Operators should not accept updates, but should instead follow the directions of fleet managers regarding update procedures

OEMs want to collect and use your data!

General Considerations

- Fleet managers should work with GSA Fleet leadership for guidance on the latest vehicle trends in the industry
- To reduce the amount of information sent to vehicle manufacturers, opt out of data tracking and do not set up accounts
- Fleet managers should review vehicle versioning for awareness and to understand what information may be going back to OEMs
- Telematics data recorded by OEMs can include images, driving patterns, location, biometric data, etc.

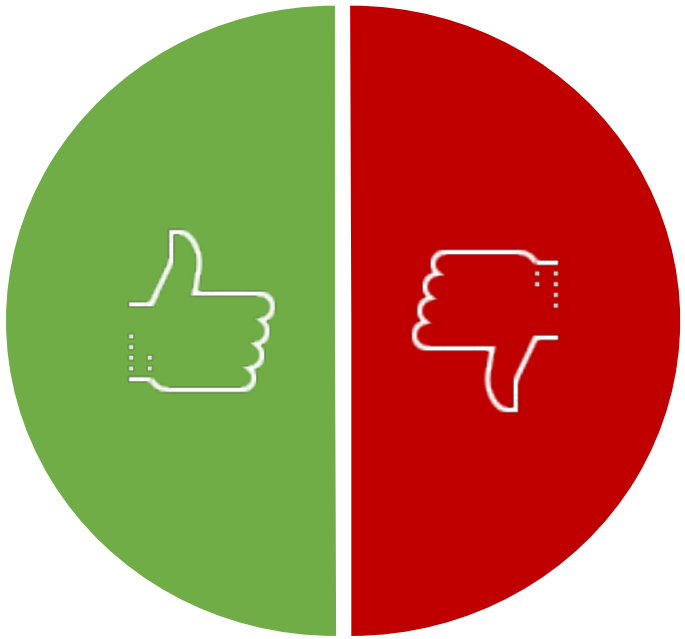
Vehicle Charging and Payment:

- Fleet operators may have the equivalent of a fleet card that works at a particular chain of gas stations. In this case, it would be a payment system that works at a particular set of charging network operators
- Training for vehicle users involves demonstrating the step-by-step process of finding an in-network charging station, plugging in, and using the payment method

Cybersecurity Best Practices

DO

- Restore/reset vehicle to factory settings
- Disable any hotspots the vehicle may have
- Delete any Bluetooth connections
- Ensure vehicle software/firmware updates are current
- Regularly change passwords to vehicle related apps
- Delete navigation history



DON'T

- Connect your phone to the vehicle through USB or Bluetooth connectors
- Ignore problems or glitches in the vehicle
- Ignore service alerts
- Accept software updates without instruction from fleet management
- Connect vehicles to unsecured wi-fi networks

Regulatory & Safety Standards

The Regulatory Ecosystem

The Regulatory Ecosystem Today

- The global connected vehicle regulatory environment is disjointed and lacks a common set of regulations, standards, and policies.
- Countries and groups of countries are either adopting some form of UN ECE guidance or have established their own regulations aimed at governing the rapidly evolving connected vehicle industry.
- There is a lack of best practices in the industry. Cybersecurity threats hit individual OEMs, and many major automakers have been hacked via their vehicles' telematics, APIs, and

What Does This Mean for GSA and the Federal Fleet Community

- The nascency of the connected car industry means that OEMs are individually developing capabilities to stay ahead of a competitive marketplace while simultaneously attempting to resist complex cybersecurity threats.
- This lack of alignment on connected car software means that individual fleet management organizations are responsible for assessing and implementing policy that guides fleet operations, management, and risk mitigation.
- While OEMs are continuing to mitigate against cybersecurity threats, vulnerabilities still exist and should be a key focal point of governmental organization
- If GSA purchases a connected vehicle and its data is being collected, that data can be retrieved by hackers

TAKEAWAY

GSA and Federal entities should proactively monitor the regulatory ecosystem to ensure that processes and controls align with the most recent thinking and best practices put forth from industry.

The United States Regulatory Environment

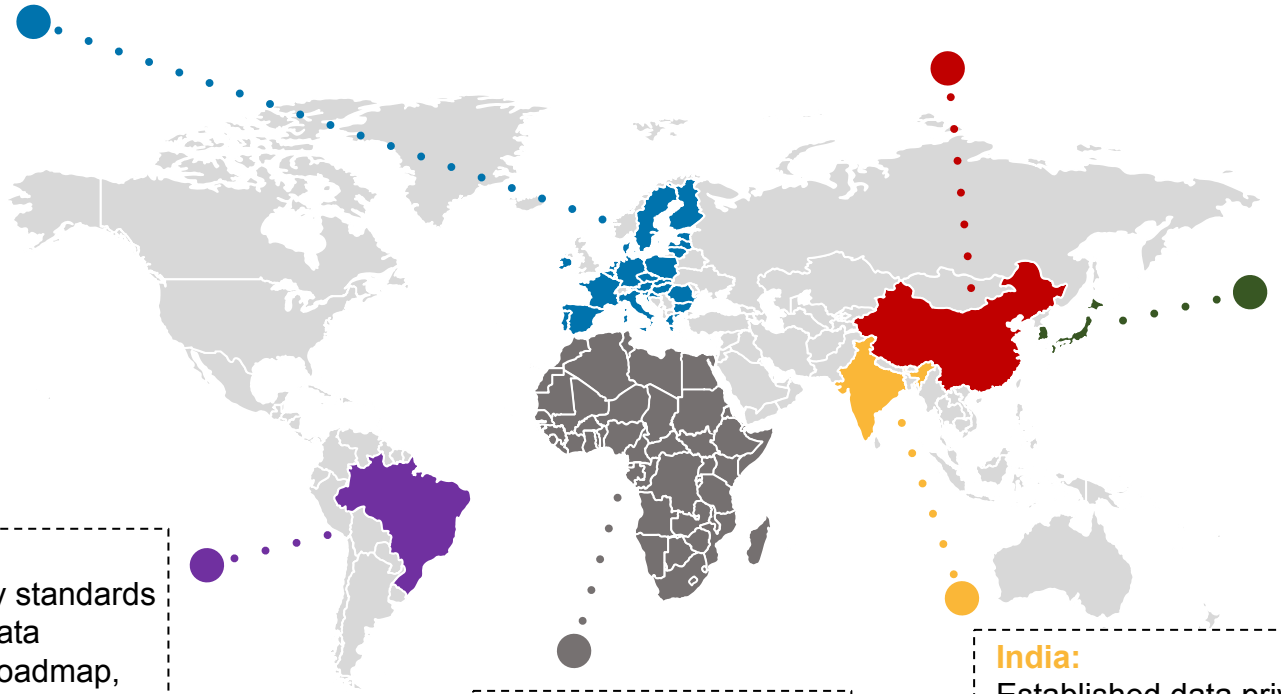
The U.S. has passed legislation that amounts to considerable financial support for EV adoption. However, the regulatory and safety environment, specifically as it relates to connected vehicles, has largely been left up to voluntary alignment with the standards developed by organizations such as SAE International (SAE) and the Institute of Electrical and Electronics Engineers (IEEE).

Impact	Description
SAE J2735 Dedicated Short Range Communications (DSRC) Message Set Dictionary:	Will assure that DSRC applications are interoperable. Applications, including collision avoidance, emergency vehicle warnings, and signage, require this standard to be effective.
SAE J2945/1 Onboard Minimum Performance Requirements for V2V Safety Communications:	Sets minimum performance requirements and interface standard features that are required to establish interoperability between onboard units for vehicle-to-vehicle (V2V) safety systems.
IEEE 1609.2-2016 Standard for Wireless Access in Vehicular Environments (WAVE) – Security Services for Applications and Management Messages:	Defines secure message formats and processing within the DSRC/WAVE system.
IEEE 1609.3-2016 Standard for WAVE – Networking Services:	Defines network and transport layer services, including addressing and routing, in support of secure WAVE data exchange. Defines WAVE short messages, providing an efficient WAVE-specific alternative to Internet Protocol version 6 that can be directly supported by applications, and the Management Information Base for the WAVE protocol stack.
IEEE 1609.4-2016 Standard for WAVE – Multi-Channel Operations:	Enhancements of the IEEE 802.11 Media Access Control to support WAVE operations and describes various standard message formats for DSRC applications.
IEEE 1609.12-2016 Standard for WAVE – Identifier Allocations:	Specifies allocations of WAVE identifiers defined in the IEEE 1609™ series of standards.

The Global Regulatory Environment

Europe:
The General Data Protection Regulation (GDPR) is in draft form, aims to establish data privacy standards for connected vehicles. The EU has also put forth draft legislation as it relates to cybersecurity (UNECE.WP.29 R155: Cybersecurity Management System) and software management regulations to govern over the air updates (UNECE WP.29 R156: Software Update Management System).

Asia:
China established the Personal Protection Information Law (PPIL) in 2021 to govern data privacy standards in connected vehicles. China has also passed Internet of Vehicles (IOV) Industry Standards for ICV Subpart 202-21 and IOV Industry Standards for ICV Subpart 202-22 to govern cybersecurity and software management standards.



Asia Pacific:
Japan (Act on Protection of Personal Information) and South Korea (Personal Information Protection Act) have passed legislation mandating data privacy standards. Japan and South Korea also abide by UNECE.WP.29 R155 and UNECE WP.29 R156 as it relates to cybersecurity management and software management.

South America:
Brazil has established data privacy standards through passage of the General Data Protection Law and has issued a roadmap, National Cybersecurity Strategy (E-Ciber), to address cybersecurity standards.

Middle East & Africa:
Has no regulations proposed or passed at this time.

India:
Established data privacy standards through passage of the Personal Data Protection Bill, but has no formal regulations as it relates to cybersecurity and software management.

Emerging Industry Trends

Emerging Industry Trends

Vehicle Manufacturer Trends

- OEMS are moving their technology to allow for greater and easier connectivity
  - Centralized computing power and zonal electrical architecture
  - These are the primary EV formats as well
- OEMs are moving more services to subscription models for connectivity and ADAS features
- Widespread adoption of the NACS Standard, retirement of CCS
  - Expands charging standardization, allows vehicles to use Tesla Supercharger network
- Cameras and sensors becoming standard in every vehicle
  - Rear Seat Monitoring
  - Driver Drowsiness and Attention Warnings
- IRA funding has spurred onshoring and nearshoring of vehicle manufacturing

Large Fleet Operator Trends

- Tracking and Monitoring
  - Fleet managers have the ability to know where a vehicle is at any time
  - Safety
  - Geofencing
- Predictive Maintenance
  - Telematics allow more knowledge of vehicles mileage, know when to replace tires, etc.
  - Fleet managers know when an indicator light activates what it means and when to fix it
- EV Infrastructure
  - Integration of on-site solar and battery storage with whole-site energy management

Resources

Training & Information Resources

Cybersecurity and Telematics Guides

- NHTSA Cybersecurity Best Practices for Modern Vehicles
- Department of Energy Federal Fleet Cybersecurity Guide
- NMFTA Freight Cybersecurity Resources
- Geotab Cybersecurity Telematics Best Practices

OEM Fleet Guides and Resources

Ford Pro

- Ford Pro Telematics Software Overview
- Ford Pro Telematics FAQs

GM Envolve

- GM Envolve 2024 Fleet Guide (pg. 11)
- GM Envolve OnStar Telematics Overview

Stellantis

- Stellantis Mobilisights Fleet Solutions
- Ram Telematics Overview

Training and Resources

Explore GSA's Inventory of Fleet Trainings and Resources:

GSA Fleet Training | GSA

Questions & Answers

- fleetsolutions@gsa.gov
- gsafleetafvteam@gsa.gov
- gsa.fleet.acquisition@gsa.gov

Fleet®