Photo Source: USDOT

# CONNECTED VEHICLES AND CYBERSECURITY


Connected vehicles are a next-generation technology in vehicles and in infrastructure that will make travel safer, cleaner, and more efficient. The advanced wireless technology enables vehicles to share and communicate information with each other and their surroundings in real time, which will help to reduce crashes, congestion, and greenhouse gas emissions.

However, as our cars become more connected (to the Internet, to wireless networks, with each other, and with our infrastructure), the risk of cyber-attacks is a growing concern.

The U.S. Department of Transportation (USDOT) understands the threat against the nation's cyber infrastructure and has made cybersecurity a top priority. The Department is taking action to respond to the threat and improve the vehicle cybersecurity posture and capabilities of the United States.

## Connected Vehicle Overview

Connected vehicles use secure and anonymous wireless technology to communicate with other vehicles, our roads, and our personal mobile devices, sharing information about their position, speed, brake status, and more and providing warnings and recommendations to drivers accordingly. These vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications will enable safety, mobility, and environmental advancements that current technologies are unable to provide. The technology is expected to reduce unimpaired vehicle crashes by 80 percent, while also reducing the 4.8 billion hours Americans spend in traffic annually.

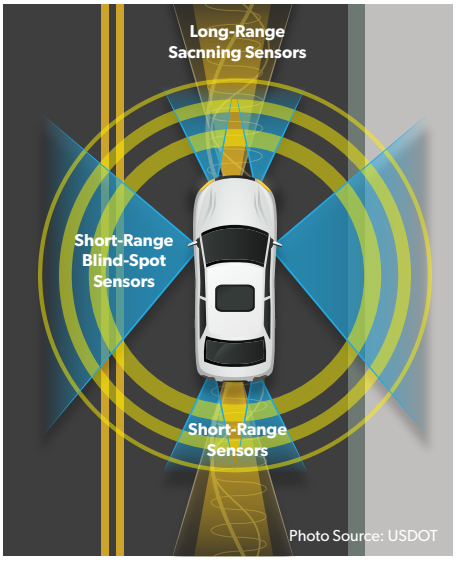

Photo Source: USDOT

The USDOT has been researching and testing this system of communicating vehicles for over a decade. The connected vehicle environment that is being researched is based on dedicated short-range communication (DSRC), which is a wireless technology that has more security and privacy protections than traditional Wi-Fi.

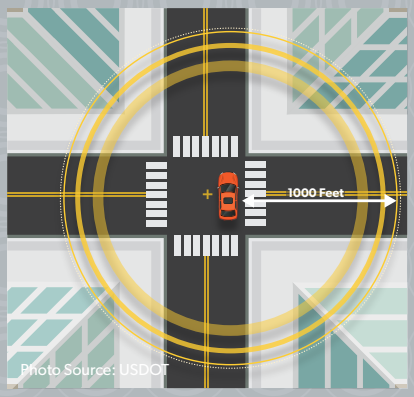

Photo Source: USDOT

DSRC has a range of only 1,000 feet, meaning cyber-attacks would require close proximity. Since safety concerns predominately involve moving vehicles, there is a very short window for attack.

U.S. Department of Transportation

## Potential Cyber-Attacks

The USDOT has adopted a "security by design" principle as it develops the system architecture for connected vehicles—meaning cybersecurity systems will be built in. The USDOT's connected vehicle architecture will encompass the entire system (not just the vehicle parts or the roadside parts), so secure uniform practices can be applied to the entire vehicle, traffic signals, work zones, and other parts of the connected vehicle ecosystem. The USDOT's vision is to apply communication security from end-to-end as a unit of data travels from one object to another. The data unit can then travel through unknown media with the assured level of security.

Potential attacks on our nation's transportation system represent hacks on products developed by private companies that do not have the end-to-end security that has been designed into connected vehicle communications nor the level of sophisticated security and cryptography.

USDOT and other research has found that Wi-Fi, infotainment service connections, and similar systems can serve as potential attack vectors for vehicle systems. Research has also shown that the impact on a vehicle's critical safety systems (steering, braking, and throttle) depends entirely on the electrical network architecture of a given manufacturer and vehicle model, trim, and year.

## USDOT Investment in Cybersecurity

From 2012 to 2014, the Intelligent Transportation Systems Joint Program Office (ITS JPO) worked with its modal partners to fund nearly $25 million in cybersecurity research to support foundational vehicle cybersecurity threat assessment and the connected vehicle program, including:

- Design, development, and operations of a security credential management system (SCMS) for the Connected Vehicle Safety Pilot in Ann Arbor, Michigan, and the continued development of an updated system that will work for 17 million vehicles and be available to use for pilots and early implementations in the 2017-to-2020 timeframe.
- Development of certification practices to check equipment prior to implementation in the Safety Pilot to ensure cyber requirements were met and the facilitation of a certification industry for the future connected vehicle environment.
- Development of best practices for handling foundational electronics control and reliability cyber threat information for the existing vehicle fleet.

Currently, the ITS JPO is pursuing early implementation of the SCMS Manager, which will operate as a gateway into the cooperative environment and grant the enrollment credentials based on proof of certification.

In addition, the USDOT continues to test and improve security architecture and cryptographic processes to accommodate advances in technology and development of the connected vehicle environment.


### What is the Security Credential Management System (SCMS)?

The SCMS is a Public Key Infrastructure-based system that ensures trusted and secure V2V and V2I communications. The SCMS employs highly innovative methods and encryption and certificate management techniques to ensure communications security between entities that previously have not encountered each other—but also wish to remain anonymous (as is the case when vehicles and drivers encounter each other on the road).

Manufacturers of devices, vehicles, or other physical components critical to a cooperative environment will have to demonstrate that they have used the correct practices before they receive the credentials that enable participation in any trusted communications.

*For more information about this initiative, please contact:*
**Walton Fehr**, Program Manager, Systems Engineering
ITS Joint Program Office | (202) 366-0278 | walton.fehr@dot.gov | www.its.dot.gov

FHWA-JPO-11-021