

Principles for a Connected Vehicle Environment

Discussion Document

www.its.dot.gov/index.htm

April 18, 2012

FHWA-JPO-12-018



U.S. Department of Transportation

Federal Highway Administration
National Highway Traffic Safety Administration
Research and Innovative Technology
Administration

This document expresses a set of working principles intended to guide U.S DOT's research, demonstration and implementation activities related to a connected vehicle environment. Connected vehicles refer to the ability of vehicles of all types to communicate wirelessly with other vehicles and roadway equipment, such as traffic signals, to support a range of safety, mobility and environmental applications of interest to the public and private sectors. Vehicles include light, heavy and transit vehicles. The concept also extends to compatible aftermarket devices brought into vehicles and to pedestrians, motorcycles, cyclists and transit users carrying compatible devices, which could make these vulnerable users more visible to surrounding traffic.

The principles in this document reflect the positions of the FHWA, NHTSA, and RITA at this time of adoption related to research, demonstration and implementation of a connected vehicle environment. These principles are subject to change in the future as the program progresses.

Purpose

- Transportation Safety is the DOT's top priority for the connected vehicle environment. The system must:
 - Prevent or mitigate the severity of crashes
 - Minimize driver workload
 - Ensure no increase to driver distraction
 - Encompass all road users
 - Ensure that mandatory safety applications cannot be turned off or overridden.
- Uses beyond safety applications, especially for mobility and environmental purposes, are permissible and encouraged as long as they do not detract from safety.

Coverage/Scale

- The system is extensible to all types of connected vehicle systems and applications (safety, mobility, environmental, etc.).
- System implementation must be national in scale and extensible across North America.
 - Implementation can start at discrete locations but is envisioned to include all major roadways with timing to coincide with the roll out of technology in vehicles.

User Protections

- DOT is committed to fostering a connected vehicle environment that ensures stakeholder and operational needs are met while at the same time protecting consumers appropriately from unwarranted privacy risks.
 - The connected vehicle environment will incorporate appropriate privacy controls: transparency; individual participation and redress; purpose specification; limitations on use of information; data minimization and retention; data quality and integrity; security; and accountability and auditing. For example:
 - The environment must provide consumers with appropriate advance notice of and, for opt-in systems, opportunity to provide consent for information collection, use, access, maintenance, security and disposal.
 - The environment will limit the collection and retention of personally identifiable information to the minimum necessary to support stakeholder and operational needs.
 - As the federal role and other critical aspects of connected vehicle regulation and/or implementation are further defined, DOT will document publicly the privacy risks and controls applicable to the system and users.
- The system must be secure to an appropriate level. The system will:
 - Ensure secure and trusted information exchange among users
 - Provide protection from hacking and malicious behavior
 - Maintain data integrity.

Implementation and Oversight

- An organization will be required to manage and operate the system responsible for ensuring security and other functions associated with the proper operation of the connected vehicle system.
 - This organization can be private, public or a private/public hybrid.
 - This organization will be governed by rules and methods of operations that ensure compliance with DOT connected vehicle principles and any other rules or requirements that may be established by the DOT with input by stakeholders.
 - All key parties will have a voice.

- Consideration should be given to allow applications from sources outside the governance structure on to the system as long as they are in compliance with all established system principles including security and operational requirements.
- The system should be implemented to provide ongoing operations.
 - If state and local agencies are involved in system implementation, the system should be designed to be cost beneficial for state and local transportation agencies in regards to building, operating, and maintaining.
 - USDOT is receptive to all sustainable financing options that do not violate other Principles. In the event that that the only viable financing option relies on financing from participating organizations, companies, or entities, the common operating costs for the system including security, governance and other costs should, to the extent feasible, be shared.
- There can be no consumer subscription fees for mandatory safety applications.
 - Does not preclude mandatory universally applicable taxes or fees to finance the system¹
 - Subscription or other fees for non-mandatory, opt-in applications are possible.

Technical Functionality

- Functionality of the system requires compliance with nationwide, universally accepted non-proprietary communication and performance standards.
 - Interoperability of equipment, vehicles, and other devices is necessary to enable mandatory safety applications as well as applications supporting mobility, economic competitiveness, and sustainability.
 - Standards must be maintained to ensure technical viability.
- The system must be technically adaptable and viable over time.
 - It must be backward compatible
 - The system must be able to evolve over time as new technologies become available.

¹ Subscription fees refer to ongoing fees that a consumer voluntarily chooses to pay for a service. Mandatory universally applicable fees differ in that they are not voluntary and are therefore likely to either be collected by government agencies (such as in conjunction with vehicle registration) or included in the purchase price of the vehicle or equipment.

- Communication technology for safety applications must be secure, low latency, mature, stable, and work at highway speeds.
 - Currently DSRC is the only known viable technology for safety critical applications.
 - DSRC or other communication technologies could be used for safety applications that are not for crash-imminent situations, mobility, and environmental applications.
- Use of the spectrum must comply with established requirements for non-interference.
 - Safety applications take priority over non safety applications.
 - Public sector applications take precedence over commercial applications.

U.S. Department of Transportation
ITS Joint Program Office-HOIT
1200 New Jersey Avenue, SE
Washington, DC 20590

Toll-Free "Help Line" 866-367-7487
www.its.dot.gov

FHWA-JPO-12-018



U.S. Department of Transportation
Federal Highway Administration
National Highway Traffic Safety Administration
Research and Innovative Technology
Administration