Overview of the Connected Vehicle Policy Program

Valerie Briggs
Team Lead, Knowledge Transfer and Policy
ITS Joint Program Office
Research and Innovative Technology Administration

April 19, 2012
Today

Safety
- 32,885 highway deaths in 2010
- 5,400,000 crashes/year
- **Leading cause of death for ages 4 to 34**

Mobility
- 4,200,000,000 hours of travel delay
- $80,000,000,000 cost of urban congestion

Environment
- 2,900,000,000 gallons of wasted fuel

Data Sources: NHTSA, CDC, TTI
Photo Source: ThinkStock
Fully Connected Vehicle

latitude, longitude, time, heading angle, speed, lateral acceleration, longitudinal acceleration, yaw rate, throttle position, brake status, steering angle, headlight status, wiper status, external temperature, turn signal status, vehicle length, vehicle width, vehicle mass, bumper height
ITS Research Program Components

Applications

Safety
- V2V
- V2I
- Safety Pilot

Mobility
- Real Time Data Capture & Management
- Dynamic Mobility Applications

Environment
- AERIS
- Road Weather Applications

Technology

Harmonization of International Standards & Architecture
Human Factors
Systems Engineering
Certification
Test Environments

Policy

Deployment Scenarios
Financing & Investment Models
Operations & Governance
Institutional Issues
Safety

Photo Source: Thinkstock
Why It Matters

Up to 80% of non-impaired crash types may be impacted by connected vehicle technology

Source: NHTSA

Based on initial estimates & studies. Actual benefits are not determined at this time.
NHTSA Agency Decision Options: 2013

**Rulemaking** on minimum performance requirements for vehicle communications for safety on new vehicles

Inclusion in NHTSA’s **New Car Assessment Program** to give car makers credit for voluntary inclusion of safety capability in new vehicles

**More research** required

Key factor will be the need for, and timing of, a **security system**

Image: istock.com
Policy Research Focus

- Determine if V2V (and V2I/V2X) is feasible to implement
  - **Security Needs**
    - Functional Requirements
    - Physical/Technical Requirements
    - Operational & Organizational Requirements
    - Financial Sustainability and Responsibility
  - **Challenges** – unique –
    - Potentially mandatory systems
    - Trip anonymity
    - Scalability, etc.
Security System: A “Must Have” for safety

Clarifications

- **Security Network** – credentialing and certificate management

- **Security Back Office** – operational functions that apply across any type of Security Network

- **Applications Infrastructure** – Infrastructure specifically for V2I safety (DSRC) or V2I mobility (other options)

All require sustainable **funding**
Security System

Security Network
Options Analysis
• Cellular/hybrid
• DSRC
• Other

Security Back Office
Functions
• Manage operations
• Certify processes & equipment
• Revocation

V2V communication via DSRC
Security System & Applications Infrastructure

Definition Underway

Applications infrastructure (via DSRC):
- Must be part of the “trusted” network
- Adhere to possible certification requirements
- Adhere to system governance

V2V communication
Via DSRC
Security System & Security Infrastructure

Applications infrastructure as a part of the security system:
- Must be part of the security network
- Adhere to performance requirements
- Adhere to system governance
- Adhere to certification requirements

V2V communication
Via DSRC
Context and Trends

Very fast moving
- Growth in consumer connectivity and the world of apps
- Emerging market “ecosystem” for apps, suppliers and, perhaps, OEMs
- Trend toward cell connection and apps in vehicles

Very slow moving
- Tight budgets for governments
- Move toward performance measures
- Emerging adoption of wireless technologies within DOTs
Main things we need to do…

- Understand and document suitable security approaches
- Understand costs
- Identify potentially viable paths for implementation
- Identify potentially sustainable financial models for supporting needs
- Understand potential risks and ramifications
- Understand stakeholder impacts, roles and responsibilities and support needs
U.S. DOT Connected Vehicle Policy Program
Organizational Structure  4/2012

ITS Management Council
DOT Leadership

V2V / Senior Policy Task Force

Implementation Policy Research & Analysis
- Financial/Partnership Models
- Security Policy – Certificate Management Entities
- Cost-Benefit Analysis
- Governance/Oversight Models
- Implementation Strategies

Technical Policy Research & Analysis
- Core System Policies
- Interface Policy Framework
- Certification Policy
- Standards/Harmonization Policy
- Spectrum Policy
- Communications Media Analysis

Legal Policy Research & Analysis
- U.S. DOT Authority
- Intellectual Property
- Privacy
- Liability/Risk Sharing
- Data Ownership/Access
- Antitrust/Spectrum
Research & Analysis Timeline: Implementation Policy Options

<table>
<thead>
<tr>
<th>CY 2011</th>
<th>CY 2012</th>
<th>CY 2013</th>
</tr>
</thead>
</table>

**Financial Modeling**
- Research Models
- Policy Analysis
- Cost Modeling

**Certificate Management Entity Organizational & Operational Models**
- Report on CME Models
- Synthesis of Results:
  - Security Cost Models
  - Infrastructure Analysis
  - Comm. Network Analysis
  - Others

**Cost-Benefit Analysis**
- Cost Modeling
- Value Propositions

**Governance/Oversight Models**
- Development of Options with Stakeholder Collaboration

**Implementation Strategies and Support**
- Synthesis of Research Results

**LEGEND**
- Research Stage
- White Paper or Presentation
- Stakeholder Review of Draft Options
Research & Analysis Timeline: Technical Policy Options

<table>
<thead>
<tr>
<th>CY 2011</th>
<th>CY 2012</th>
<th>CY 2013</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Communications Network Analysis</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Assess and Model Options</td>
<td>• Evaluate/Compare Options</td>
<td>Draft of Viable Options Final Report on Viable Options – Results inform Financial/Partnership Models</td>
</tr>
<tr>
<td><strong>Infrastructure Analysis</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Infrastructure Analysis Results</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Core System Policies</strong></td>
<td>• Stakeholder Analysis</td>
<td>• Core System Policy &amp; Institutional Analysis</td>
</tr>
<tr>
<td><strong>Interface Policy Framework</strong></td>
<td></td>
<td>• Policy Framework</td>
</tr>
<tr>
<td><strong>Standards &amp; Harmonization Policy</strong></td>
<td>• Core System Interface Inventory</td>
<td></td>
</tr>
<tr>
<td><strong>Certification Policy</strong></td>
<td>• Policy and Institutional Analysis</td>
<td>Drafting of Criteria for Certification Policies</td>
</tr>
<tr>
<td><strong>Spectrum Policy</strong></td>
<td>• Analysis of Spectrum Management Policy</td>
<td></td>
</tr>
</tbody>
</table>

**LEGEND**

- Research Stage
- White Paper or Presentation
- Stakeholder Review of Draft Options

NHTSA Agency Decision (HV) 2014
Continued Efforts based on Results
Draft Harmonization Policies
Draft Control/Access Policies
Draft Standards Policies
Draft Certification Policies
Draft Spectrum Policies

U.S. Department of Transportation
Principles: Purpose

- Transportation safety is the DOT’s top priority.

- The principles require that the system:
  - 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 are permissible and encouraged as long as they do not detract from safety.
Principles: 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.
Principles: 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.
Principles: User Protections (continued)

- 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.
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 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.
Principles: Implementation and Oversight (continued)

- 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 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.
Principles: Implementation and Oversight (continued)

- There are no consumer subscription fees for mandatory safety applications.
  - Does not preclude mandatory universally applicable taxes or fees to finance the system**
  - Subscription or other fees for non-mandatory, opt-in applications are possible.

**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.
Principles: 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
  - Must be backward compatible.
  - System must be able to evolve over time as new technologies become available.
Principles: Technical Functionality (continued)

- 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.
For More Information

www.its.dot.gov