Connected Vehicle Policy Program

Valerie Briggs, ITS JPO
September 25, 2012
Chicago, IL
USDOT Connected Vehicle Policy Program
Organizational Structure  9/2012

ITS Management Council
DOT Leadership

Senior Policy Task Force

Implementation Policy Research & Analysis

Technical Policy Research & Analysis

Legal Policy Research & Analysis
Security Credential Management System (SCMS)

SCMS represents the entire system, and CMEs house the functions

Certificate Authority

Registration Organization
- Linkage Authority 1
- Registration Authority

OBE and Infrastructure

LEGEND
- = TBD
- = Function
- = Certificates
- = Keys
- = Certificate Management Entity
Different organizational models are being considered for the system
Current analysis based on new design
Major cost drivers of SCMS:
  – Hardware and software needs (~50-60% of total costs)
  – Numbers of physical locations of functions and organizations
  – Choice of organizational model – oversight, management, and efficiency
Various ownership options being analyzed
  – Public-private partnership, all private
  – Will impact organizational models and costs
If or how PII may be collected as part of registration into the system is being analyzed
Internal controls and policies needed to protect security and privacy are being analyzed
Communications System for Security

- Four scenarios:
  - Mostly cellular system
  - Mostly cellular with some installation of DSRC RSE
  - “All DSRC”
  - CAMP Phased Deployment Scenarios

- Three principal cost drivers:
  - On-Board Equipment (OBE) is a significant in-vehicle cost in all scenarios
  - Road-Side Equipment (RSE) is a significant infrastructure cost in an “All DSRC” scenario
  - Cellular may be a significant cost in those scenarios that rely on it for certificate delivery
Communications System for Security

- Delivery of the Certificate Revocation List (CRL) is expensive and technically demanding

- With incremental or no CRL delivery:
  - Certificate Authority maintains CRL, but does not distribute. Instead, certificates are withheld from misbehaving vehicles.
  - Cellular data costs drop substantially.

- With no CRL distribution, OBE costs are the most expensive part of the system:
  - OBE costs vary slightly for each scenario due to cost and power consumption of subcomponents
  - OBEs are necessary for safety, so the incremental costs to serve the function of communicating to the SCMS are relatively small
  - Results are very sensitive to inputs; uncertainty in conclusions is high
Communications System for Security

- For an “All DSRC” scenario, the number of RSEs nationwide depends on risk tolerance and coverage requirements:
  - Estimates vary from 1300 RSEs to 150,000 RSEs
  - Unanswered Questions:
    - What level of coverage is acceptable?
    - How frequently must a vehicle interact with the system?
- Lowest cost scenario hinges on number of RSEs required
  - Cellular scenarios are lowest cost if “All DSRC” requires many RSE
  - OBE costs become most important if “All DSRC” requires fewer RSE
Communications System for Security

- Operational issues and unknown variables dramatically impact costs of cellular options
  - Cellular scenario highly sensitive to changes in the misbehavior rate, CRL variable data size, and peak prices

- Installation, operation and maintenance of RSE’s pose significant challenges for DRSC options
  - Placement of RSE’s in state or locally owned equipment cabinets and rights-of-way would require a significant implementation permitting, coordination and system integration effort
  - Placement of RSE on private property may be an alternative but would also require a strategy for implementation
Other Implementation /Technical Policy Issues

- Business Models
- Infrastructure Analysis - AASHTO
- Spectrum
- Core System Architecture Analysis
- Standards and Certification Needs Identification
Legal Policy - Scope of Authority

- NHTSA has authority to support:
  - Key aspects of V2V communications
  - Regulation of critical equipment, messages and applications if related to safety
  - Provision of the security required to support a V2V rule by a non-Federal entity, as through a procurement or other form of agreement or indirectly via a V2V regulation

- FHWA does not have authority to require installation of roadside infrastructure
Other Legal Policy Issues

- Intellectual Property

- Privacy
  - Need to distinguish between trip-trackability and ability to identify bad actors on the system
  - DOT will do comprehensive review of any final system and involve appropriate privacy community