RITA Intelligent Transportation Systems Joint Program Office

Enabling a Secure Environment for Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) Transactions

April 2012 Public Workshop Proceedings

Proceedings – June 2012
www.its.dot.gov/index.htm
FHWA-JPO-12-072

U.S. Department of Transportation
Research and Innovative Technology Administration

Produced by Booz Allen Hamilton for
ITS Joint Program Office
Research and Innovative Technology Administration
U.S. Department of Transportation

Notice

This document is disseminated under the sponsorship of the Department of Transportation in the interest of information exchange. The United States Government assumes no liability for its contents or use thereof.

Technical Report Documentation Page

1. Report No. **FHWA-JPO-12-072**	**2. Government Accession No.**	**3. Recipient's Catalog No.**
4. Title and Subtitle Enabling a Secure Environment for Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) Transactions April 2012 Public Workshop Proceedings		**5. Report Date** June 8, 2012 **6. Performing Organization Code**
7. Author(s) Andrea Waite, Richard Walsh, and Dominie Garcia		**8. Performing Organization Report No.**
9. Performing Organization Name And Address Booz Allen Hamilton 8283 Greensboro Drive McLean, VA 22102		**10. Work Unit No. (TRAIS)** **11. Contract or Grant No.** **DTFH61-11-D-00019**
12. Sponsoring Agency Name and Address Research and Innovative Technology Administration Intelligent Transportation Systems, Joint Program Office 1200 New Jersey Ave SE Washington, DC 20590		**13. Type of Report and Period Covered** Formal Deliverable, April 19-20, 2012 **14. Sponsoring Agency Code**

15. Supplementary Notes

16. Abstract

This report provides a summary and overview of the Public Workshop entitled, "Enabling a Secure Environment for Vehicle-to-Vehicle and Vehicle-to-Infrastructure Transactions", presented by USDOT. The workshop took place on April 19-20, 2012 at the Capital Hilton in Washington, D.C. and was intended to bring together various public and private stakeholders interested in the connected vehicle program to provide updates on the program's progress and related policy work. The workshop included discussion of the communications security architecture and design under development, and provided an opportunity for solicitation of input related to additional critical areas of analysis. Multiple breakout sessions were held to discuss business model frameworks, and operational and implementation considerations. Key take away points from those sessions and plenary sessions are included in this proceedings document.

17. Key Words Certificate Management Entity, Communications Data Delivery System, Dedicated Short Range Communications, Vehicle-to-Vehicle, Vehicle-to-Infrastructure, Public Key Infrastructure	**18. Distribution Statement**		
19. Security Classif. (of this report) Unclassified	**20. Security Classif. (of this page)** **Unclassified**	**21. No. of Pages** 28	**22. Price**

Form DOT F 1700.7 (8-72) **Reproduction of completed page authorized**

Table of Contents

Executive Summary

Introduction

On April 19-20, 2012, the Intelligent Transportation Systems Joint Program Office (ITS JPO) within the U.S. Department of Transportation's (USDOT) Research and Innovative Technology Administration (RITA) hosted a public meeting entitled: *Policy Research Workshop on Enabling a Secure Environment for Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) Transactions.* This two-day workshop provided an opportunity for information exchanges between connected vehicle stakeholders and the USDOT. Individuals involved in connected vehicle research presented research results to date relating to institutional model options for V2V and V2I communications security. Approximately 100 stakeholders attended the workshop in person, and an additional 30 stakeholders took part in the webinar.

The workshop took place during the mid-point of two related policy research projects – one focused on the institutional models for communications security and approaches to back end security processes, and another focused on network options for communications systems. Feedback from the workshop will inform the completion of both projects, for which final documents and briefings will be available later in 2012.

Workshop Objectives

The objectives of the workshop were to:

- Update stakeholders on policy work for the connected vehicle research program.
- Update stakeholders on analysis performed to date to identify options to support communications security needs, including back end processes and alternative network options.
- Solicit input from stakeholders on critical areas of analysis, including business models and operational considerations.
- Provide opportunities for stakeholders to articulate concerns and challenges for anticipated implementation.

Key Take Away Points

Summary of Key Take Away Points from Day 1 Breakout Sessions

The following points resulted from discussions during the "Business Model Framework Considerations" track:

- Awareness of the connected vehicle concept and its value proposition is lacking. Awareness is a critical basis for making the case for funding requests.
- Non-safety applications can help drive implementation of the system if they are valued by potential users; applications must provide valued information, not simply data, to users.
- Funding for and investment in applications requires data collection processes that enable dissemination and cutting edge concepts to be realized. Once such cutting edge concepts emerge, they will help lead to the emergence of revenue streams.
- Potential investors desire to be assured that there is a market for connected vehicle applications.

The following points resulted from discussions during the "Operational and Implementation Considerations" track:

- Numerous outstanding issues still exist related to the technical specifications of the system.
- Stakeholders desire to explore the specific details of how privacy will be protected in the system.
- Implementation can follow different paths. Participants noted that implementation will ultimately depend on federal government decisions as well as decisions about the ultimate ownership structures of the CMEs.

Summary of Key Take Away Points from Day 2 Breakout Sessions

The following points resulted from the discussions on System Deployment:

- Rolling out roadside infrastructure comes with a significant cost, one that most state and local agencies are not prepared or able to handle.
- Although parts of the European model could work for the U.S. (a model that is significantly based on connected vehicle mobility applications), considerations regarding the types of applications and the need for protecting users' PII should be kept in mind, as European Union policies are different from those in the U.S.

The following points resulted from the discussion on System Ownership:

- Approaches such as "public-public-private partnerships" could be further explored.
- Public-private partnerships do exist today, but they require strong leadership and clear delineation of responsibilities.

- The relationship between the state and federal governments in the context of the connected vehicle system should be clarified because as time progresses stakeholders will need to understand their responsibilities as well as where efforts and resources should be directed to have the greatest impact.
- Privacy of users in the system is a sensitive topic that is being considered throughout the research.

Chapter 1. Public Workshop Overview

Introduction

On April 19-20, 2012, the Intelligent Transportation Systems Joint Program Office (ITS JPO) within the U.S. Department of Transportation's (USDOT) Research and Innovative Technology Administration (RITA) hosted a public meeting entitled: *Policy Research Workshop on Enabling a Secure Environment for Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) Transactions*.[1] The workshop gave participants an opportunity to learn about and provide input into research being conducted on potential organizational and business models for supporting communications security and data exchange needs for V2V and V2I crash avoidance and other applications.

The workshop took place during the mid-point of two related policy research projects – one focused on the institutional models for communications security and approaches to back end security processes, and another focused on options for network communications systems. A key challenge for the V2V and V2I infrastructure is establishing a secure, trusted data exchange among vehicles and other equipment. Current research is focused on better understanding system needs and the implications of alternative approaches. Feedback from the workshop will inform the completion of both projects, for which final documents and briefings will be available later in 2012.

Workshop Details

The Public Workshop took place at the Capital Hilton in Washington, DC. Approximately 100 individuals joined the workshop in person while another 30 joined via webinar. The workshop structure was focused on breakout sessions for discussing critical issues and obtaining feedback from stakeholders. Participants were provided with read ahead materials for both research projects, and representatives from these projects presented an overview of work completed thus far as well as a discussion of outstanding issues and next steps. These materials have been posted for a limited time online at the following web address: http://www.its.dot.gov/meetings/v2v_meeting.htm.

Presentations were made by staff from the National Highway Traffic Safety Administration (NHTSA), Federal Highway Administration (FHWA), Vehicle Infrastructure Integration Consortium (VIIC), and American Association of State Highway and Transportation Officials (AASHTO) who are leading connected vehicle research. For a limited time, all presentations are available at: http://www.its.dot.gov/presentations.htm.

[1] 'USDOT Announces Public Meeting on Enabling a Secure Environment for Vehicle-to-Vehicle and Vehicle-to-Infrastructure Transactions,' http://www.its.dot.gov/meetings/v2v_meeting.htm (May 2012).

Representatives from various stakeholder groups attended the workshop and provided their feedback and insights on the topics discussed. A list of the stakeholder groups represented by the attendees includes:

- State and local departments of transportation and transit agencies
- Automotive manufacturers and suppliers
- Trucking industry
- Commercial cellular, telecommunications, and IT companies
- Transportation and technology consultants
- Associations and interest groups representing these industries

Workshop Objectives

As described above, this workshop gave representatives engaged in connected vehicle research an opportunity to update stakeholders and elicit stakeholder discussions on concerns or areas of interest that require additional study. The objectives of the workshop, which are summarized in the Agenda (see Appendix A), were to:

- Update stakeholders on policy work for the connected vehicle research program.
- Update stakeholders on analysis performed to date to identify options to support communications security needs, including back end processes and alternative network options.
- Solicit input from stakeholders on critical areas of analysis, including business models and operational considerations.
- Provide opportunities for stakeholders to articulate concerns and challenges for anticipated implementation.

Chapter 2. Day 1

Plenary Session

The workshop began with a welcome from the Deputy Administrator for RITA, Gregory D. Winfree. Setting the tone for the workshop, Mr. Winfree articulated the need for innovative thinking about business models and implementation. Providing stakeholders with information and soliciting input and ideas were also central themes in his opening address.

The morning session included several other presentations designed to provide background information on current research projects within the connected vehicle program. These presentations are available for a limited time on the ITS JPO website at http://www.its.dot.gov/presentations.htm and are outlined here:

- **Overview of the Connected Vehicle Policy Program** – Valerie Briggs, Team Lead, Knowledge Transfer and Policy, RITA ITS JPO
    - Ms. Briggs gave an overview of the connected vehicle program and presented on how connected vehicle technology could assist in increasing safety on our roadways. She reviewed the focus and challenges of the connected vehicle program, discussed the need for communications security for V2V and V2I systems, and presented results to date on related policy research activities. She concluded her presentation by talking about the principles that the USDOT has developed to guide its work on the connected vehicle research program.
- **Connected Vehicle Legal Policy Work** – Dana Sade, Senior Counsel, NHTSA
    - Ms. Sade spoke about legal and policy issues stemming from the connected vehicle environment, including current USDOT authority relevant to implementing V2V communications and the extent to which NHTSA authority may extend to connected equipment, technologies, and messages.
- **Infrastructure Perspective** – Robert Arnold, Director, Office of Transportation Management, Office of Operations, FHWA
    - Mr. Arnold provided the FHWA's perspective on the connected vehicle program, which includes a strong interest in the V2I applications. He discussed FHWA's authority to support connected vehicle implementation and the role of the Federal-Aid Highway Program. He noted the increasing focus on performance measurement and safety improvements in state DOTs as potential motivators for state and local agencies to choose to install connected vehicle infrastructure.
- **Security and Privacy, Understanding the Prototype V2V Safety Security Design** – Tom Schaffnit, Honda R&D and President of VIIC
    - Mr. Schaffnit reviewed the technical approach to communications security that was developed by representatives of the auto industry and security experts. He

emphasized the importance of communications security and reviewed the goals, scope, limitations, back end functions within the system, and questions remaining for further study.

- **Operational and Organizational Models for Certificate Management Entities (CMEs)** – Dominie Garcia, Associate, Booz Allen Hamilton
    - Dr. Garcia spoke about the organizational and institutional analysis for Certificate Management Entities (CMEs) including a discussion of the back end functions, industry standards for protecting security and privacy, and cost estimation approach and cost impacts. She also noted the outstanding decisions that need to be made in order to complete the analysis of CME models.
- **High Level Options for Secure Communications Data Delivery System** – Jim Misener, Executive Advisor, Booz Allen Hamilton
    - Mr. Misener spoke about the analysis conducted to identify options for the Communications Data Delivery Systems (CDDS). His discussion reviewed the four high level options for the CDDS; the advantages and disadvantages of each; the technical and commercial components, which also included financial elements; and different communication types.
- **Mobility Applications for Connected Vehicle Data: Policy Workshop** – Brian Cronin, Team Lead, Research, RITA ITS JPO
    - Mr. Cronin provided an overview of the Basic Safety Message (BSM) and how the BSM data elements support the high-priority dynamic mobility applications. His presentation focused on the BSM fundamentals and next steps for BSM analysis that is being conducted by the connected vehicle mobility program.
- **Core System Stakeholder Analysis** – Volker Fessman, Research Transportation Specialist, FHWA
    - Mr. Fessman presented on the concept of the connected vehicle core system. A core system is envisioned as a key element in supporting secure and trusted data exchange among the traveling population and transportation entities that have no previously established relationships to one another. His presentation provided some details regarding what comprises a core system. He also noted the relevance of such systems to stakeholders by offering a set of short case studies that describe the opportunities to be gained by agencies that participate or own a core system, by emergency responders, by electronic tolling/payment facilities, and others.
- **Connected Vehicle Application and User Needs: AASHTO Perspective** – Jim Wright, Program Manager, AASHTO
    - Mr. Wright discussed the Infrastructure Deployment Analysis conducted by the States that identified priority connected vehicle applications for state and local agencies, which includes safety and speed advisories, among others. Mr. Wright also discussed the actions taken by states and their current positions on infrastructure investments, and states' projected deployment scenarios for 2012-2025.

After the plenary sessions in the morning, the afternoon was organized around two separate discussion tracks: "Business Model Framework Considerations," and "Operational and

Implementation Considerations." All workshop participants were able to attend each track and engage in discussion with a small group.

Track 1: Business Model Framework Considerations

The "Business Model Framework Considerations" track was designed to gather feedback from stakeholders about the issues surrounding potential applications for the connected vehicle system and ideas for revenue generation that could offset system costs. These discussions included numerous related discussions about benefits, funding challenges, and opportunities for commercialization, among other topics. The facilitators for these sessions were Dr. Dominie Garcia and Dr. Chris Hill. Following is a combined summary of the predominant issues and points discussed in both breakout sessions as well as key take away points for business model framework considerations.

Discussion of Applications

The breakout session began with a discussion of high-value connected vehicle applications in general and gradually narrowed to focus on specific areas of concern. The focus on non-safety applications in this session was aimed at facilitating an idea-generating discussion about ways in which costs for the build out and operation of the system may be potentially offset. Research and development of opt-in applications that can be monetized has already begun, and soliciting input from stakeholders on feasibility and value across the connected vehicle system was done to further inform future research into business model scenarios.

When speaking about the different capabilities of applications, participants made the point that the focus should not be on the data, technologies or processes, as it is *the information that is the commodity that can potentially be leveraged*. The system has the ability to allow users to access information in new ways. There was broad discussion of numerous examples of applications, including:

- Parking applications for drivers and municipalities
- Origin-destination trip information for state and local agencies
- Mobile weather applications for pavement condition management by state DOTs
- Localized advertisements from businesses to nearby drivers
- Traffic volume management during high volume events (e.g., sporting events, concerts)

Participants spoke of applications in two broad categories – those applications that *increase safety* and those that *provide potential for revenue generation*. Several stakeholders noted that the benefits of safety systems are diffuse, and not necessarily directly linked to the purchaser.

Prioritization of applications was difficult for participants. Several stakeholders stated that the *safety applications would certainly rank higher in importance for implementation;* however, others noted that *investors would likely be more interested in mobility applications and advertisements* and it may be difficult to entice investors to build out or maintain the systems needed *just* for safety applications. It was noted that any application should be evaluated based on the potential level of interest in the market. For example, some representatives from state DOTs voiced an interest in origin-destination trip information from drivers in their road systems in order to identify problem areas where additional

support is needed, but other stakeholders mentioned that, ultimately, there isn't a huge market of public sector agencies buying data.

Below is a synthesis of key take away points from the stakeholder discussion concerning applications:

- Non-safety applications can help drive the implementation of the system if they are valued by potential users.
- Non-safety applications can potentially generate revenue.
- Stakeholders believe NHTSA/FHWA should define guidelines for application development (e.g., if advertisements are not acceptable due to distraction/bandwidth concerns, this must be made clear).
- Non-safety applications must go beyond providing just "data" – "information" and "knowledge" are what drivers and other potential customers want (e.g., state DOTs looking for origin/destination information).
- Future connected vehicle applications need to be distinguished from what currently exists.

Ongoing Revenue and Funding Ideas

Evolving from the discussion of potential applications was a conversation about sources of revenue and commercial applications that may induce private organizations to finance parts of the system. Many participants believed that it is unlikely that a single application will drive the success of the program and generate adequate revenue. Instead, *a combination of many marginally productive applications taken together would more likely represent the system revenue generation model*. The participants took this idea a step further and asserted that the distribution of revenue sources may make it less likely that a single private entity would act as a sole investor in the system, implying the need for exploration of various partnerships and alliances, either between multiple private organizations or between public and private organizations.

Key take away points from the stakeholder discussion concerning ideas for ongoing revenue and funding include the following:

- Potential investors need to be assured that there is a market for connected vehicle applications.
- The value of applications is likely to be seen in small pockets, with several marginally productive opportunities.
- Since public funding tends to be segregated by program, any funding from state agencies for the connected vehicle system should be associated with an existing state program (e.g., safety, mobility, operations).
- It is likely that applications would have to compete for funding from state and local agencies with traditional safety investments, so evidence of benefits is necessary to make a case for funding.

Initial Investment Considerations

There was a significant discussion around initial sources of funding for the build out and implementation of connected vehicle systems and technologies. While several stakeholders were curious about the potential for federal funding, the conversation was redirected to brainstorm about alternate sources, such as non-federal public agencies or commercial organizations. The following points represent the key take away points in the discussion about state funding:

- *The importance of paying close attention to states' preferences cannot be understated*, especially in terms of benefits related to traffic management. Participants noted that if a state was expected to pay for the system in any way, its priorities should be taken seriously.
- The value proposition must be clarified for the public sector, especially in terms of the cost saving benefits that can be seen over time – this is what will influence decision makers.
- Additional studies need to be conducted with solid data that illustrates how a state agency would benefit from the connected vehicle system, perhaps through future cost reductions and budget savings. Participants noted some examples. For instance, an agency might save funds if connected vehicle traffic management applications could be used to reduce traffic and congestion and thus decrease some of the anticipated future investment in a state's highways. Another example would be if agencies could substitute connected vehicle technologies for existing infrastructure or field devices, such as dynamic messaging signs.
- The way in which funding is planned and allocated for agency or state funded programs should be considered. Stakeholders noted that connected vehicle implementation and operations might creatively use different funding programs in such areas as state-based safety programs, air quality programs, or funding for ITS and operations.
- Because of the structure of the transportation planning process, participants noted that connected vehicle applications would have to compete for funding with current safety initiatives and countermeasures, which again resulted in a discussion about the critical need for analysis of the value proposition as a basis for funding proposals.
- Ultimately, the system must be framed within the existing funding channels at the state level and backed by solid analysis to convince decision makers and politicians that it is a worthwhile investment.

Several stakeholders expressed *the belief that the NHTSA decision (scheduled for 2013) would determine who would invest in the system and when*. Stakeholders thought that under a scenario of mandated participation in the system, commercial investors may be more inclined to develop and release non-safety applications because of assurance of large numbers of users.

In response to the discussion about commercial organizations that may be interested in releasing applications, the facilitators urged participants to consider the possibilities for investment in the system build up and revenue generation separately from the NHTSA decision. A few key points that came out of that discussion include:

- It is difficult for many stakeholders to envision how extensive the connected vehicle system will be at various levels of deployment, and to understand how much additional bandwidth will be available for non-safety applications.

- There is uncertainty about whether or not the payback for the system needs to be seen on day one of the roll out. Many stakeholders felt that some immediate benefit is needed to engage both drivers and investors.
- "Who benefits?" is a difficult question to answer because the benefits may not be evenly distributed across participants. In an opt-in scenario, one driver's investment could benefit another driver.
- A set of enticing applications may spark an interest in the system that will be critical to ensuring that initial investment occurs and that an immediate benefit is felt by users.

Phasing and Roll Out

A foundational point in this discussion was that many participants believe that *there is a lack of understanding of the connected vehicle environment concept among the private sector and state and local agencies*. Some believe that there is almost no awareness of the program at the local level. Participants emphasized that it is an important issue to consider in tandem with the development of scenarios that describe a phased approach to implementation, as a measure both of creating awareness *and* gaining greater support among local agencies and commercial organizations.

When participants were prompted to discuss feasible business models, they reflected on the European model. The model in Europe is envisioned to roll out incrementally over several years, and is focused on soft safety and eco-driving applications that have a visible impact to the driver in real-time; it is not as comprehensive as what is envisioned with the U.S. connected vehicle environment at full deployment. Because of these differences, participants were not clear on what can be learned from this model, but encouraged the USDOT to do further investigation.

Stakeholders from OEM groups emphasized the importance of having some initial field infrastructure (e.g., some roadside units or signal phase and timing messages) so that early adopters of the system can have at least a basic level of V2I interaction.

Lastly, it was suggested that transit authorities, private sector fleets, and public safety agencies be considered as potential candidates for an initial roll out group. These groups could not only test the technologies and realize benefits such as congestion monitoring and re-routing, but also would familiarize the public and potential users with the system for future phases of roll out. For example, if transit agencies deployed connected vehicle technologies, transit users would benefit from the various applications and uses and could then be educated about the value of the underlying connected vehicle system, thus evolving the population base of support through wider understanding of the system and its benefits.

An additional take away point related to the idea of a phased implementation is that the program is lacking some key details about requirements and cost structures would be necessary to address concerns of private sector partners. Because of the predominant nature of public sector participants at the workshop, it was acknowledged that there are likely additional concerns within the private sector not captured during the workshop.

Track 2: Operational and Implementation Considerations

The second breakout session focused on operational and implementation considerations for the network and communications security back office services. The topics in this section included technical questions about the communications system architecture, the length of time it would take to set up the network, the implementation needs for both initial and national scale deployment of systems and infrastructure, what coverage priorities should be, and key challenges for setting up the network. The facilitators for the Operational and Implementation Considerations sessions were Mr. Jim Misener and Mr. John Collins.

Technical Questions about the Communications System Architecture

To begin this discussion, participants were asked if they thought anything was missing from the morning presentation regarding the various network scenarios and wireless links. The discussion resulted in participants talking about:

- Back up communications systems
- Which cellular companies ought to be engaged in the discussion going forward
- What (if any) is the probability of failure rate of any of the wireless links

Participants were curious about risk identification and risk mitigation during the planning process. For example, several stakeholders asked whether or not *significant failures are being reviewed and evaluated*. Significant failures can include a network collapse, power outage, or unanticipated system down-time.

The participants were then asked if they had any expectations about the evolution of communications security and privacy protection as the system evolves. Key take away points from this discussion include:

- There is a potential for third parties to create cell phone applications for safety; is regulation of such applications important? What can and should be done?
- Participants voiced concerns about: *congestion of cell phone and bandwidth, multiple applications running at the same time, and the right of service providers to know if safety applications are being used*.
- Additional *liability concerns remain for opt-in applications*; and some participants argued for appropriate oversight of opt-in applications.
- When participants were asked how long it would take to set up a system based on different scenarios/models and timing and phasing of roll out, many stated that *there is no way to predict how long the infrastructure and communications network will take to be set up* as total system needs have not yet been determined. Participants seemed to be in agreement about an expectation that it would take up to 20 years for the system to reach 95% penetration.

Based on the discussions about outstanding technical issues and specifications, some key take away points are:

- Backwards compatibility of OBE technology is critical; OBE must last for the lifetime of a vehicle and should have additional memory/capacity to handle future expansion of functionality, so as to avoid a burden on users (requiring updates) and to ensure that participation in the connected vehicle system is as high as possible.
- Some stakeholders advocated for a longer than five minute certificate lifespan (at least initially) or a lifespan not associated with a specific time interval due to the impact that a short-lived certificate has on the size and load required of the security system. Related to this topic are several questions that still need additional technical analysis including:
  - What is the impact of changing the current five minute specification?
  - Is it technically feasible to have varying degrees of certificate lengths on the system at the same time – either through a phased approach, different time lengths according to trip length, or different lengths according to user's comfort and opt-in to different levels of privacy/security?
  - If it is technically feasible, what would be the implications be on privacy and communications security?
- Specification of the impact of long-term "fall back" certificates is still needed.
- There is a need for planning and estimation of how redundancy and risk identification and mitigation are built into the system.
- Additional analysis and design of the misbehavior process is necessary to address issues regarding global processing and how misbehavior is identified, as well as certificate revocation lists, how they are managed, and when and how they are distributed.

Implementation Considerations

Participants were asked what is required to get started with implementation. The groups first stated that *they would be more confident about the value of the system and thus interested in investment and resource allocation for deployment of the system if it had well-defined goals*. Without well-defined goals, participants believe that it will be difficult for their respective organizations (either public or private) to justify large investments.

Participants also discussed how *hardware and software should have* more memory or capabilities than needed at initial deployment to allow for future updates. One stakeholder reported that a coalition of auto manufacturers in Europe is exploring the possibility for jumpstarting connected vehicle deployment by pre-loading two years-worth of certificates onto vehicles. Alternative provisions for security would need to be made once those certificates expire. The stakeholders recommended that the USDOT consider researching the European system further.

The participants also discussed their perception of coverage priorities (e.g., urban, suburban, rural, etc.). A key take away from this discussion is that *where the roll out begins will directly depend on who owns the system*.

- If the system is government-owned, the system will likely be rolled out in areas with high levels of fatal car crashes.
- If the system is privately owned, the system will likely be rolled out in urban areas first. Urban areas would precede rural areas because of the density of the population, the opportunity to realize greater levels of commercial benefits, and the ability to test the

technology with large numbers of users. This is similar to the roll out of telephone networks. For example, cell phone companies usually put up infrastructure in more dense urban areas before moving to rural areas since deployment is more expensive in rural areas; participants agreed that this provides a strong example or model for the deployment of the connected vehicle program.

- In addition, urban areas represent a greater opportunity to educate users about the value of the system and test new applications, system technologies, and network capabilities.
- A suggestion was that drivers should have the ability at first to opt-in to mobility applications, and then safety benefits would be realized later.
- Non-uniform software update policies should be considered for urban and rural areas so that certificate refresh can occur on a schedule that is appropriate for the area.

Participants also discussed the impact of future USDOT or NHTSA policies, and articulated some desires for guiding policies to help influence roll out and continuity within the system. Key take away points from these discussions include:

- Many participants perceive a need for a standardized OBE, perhaps an "ITS Certified" stamp on all equipment associated with the connected vehicle system. If there is a government mandate, stakeholders expressed the desire to see minimum performance standards rather than design standards.
- Stakeholders noted that there is no easy path to use DSRC for certificate distribution and management functions. One stakeholder expressed a limited need for DSRC on freeways due to the existence of other probe data collection capabilities currently available. For a DSRC based RSE to be used for security, backhaul communications to the certificate management entity would be necessary and could present a significant implementation hurdle in many areas.
- Participants encouraged consideration of an approach being considered in Europe for initiating connected vehicle capabilities, with the following characteristics:
  - Voluntary (i.e., opt-in) participation
  - Pre-load security certificates on OBE for two years (another security solution would need to be established before the two years expired to continue benefits)
  - Life cycle of certificate is based on an ignition cycle (it is used when the vehicle is turned on only), which would allow trackability by trip.

A brief discussion regarding the size and frequency of Certificate Revocation Lists (CRLs) and the lifespan of certificates also took place. The group agreed that *cellular would be a good option for CRL distribution* and that further research was needed on an appropriate lifespan of certificates to ensure safety and privacy.

Day 1 Closing Session

After each breakout session was completed, participants were asked to fill out feedback surveys about the topics covered and outstanding issues that they wanted to explore in more depth. These surveys were used to design the agenda for Day 2. Upon completion of the final breakout sessions, all participants returned to the main conference room. Ms. Briggs provided concluding points about the Day 1 sessions and reviewed the schedule for Day 2.

Chapter 3. Day 2

Day 2 Opening Session

Day 2 began with a short summary of the Day 1 discussions. Based on the outcomes from Day 1, two additional breakout sessions were created to delve deeper into topics of interest to stakeholders – one focused on system deployment and the other on system ownership issues. Participants were invited to choose which breakout session to attend.

Day 2 Breakout Session: System Deployment

The objective of the system deployment breakout session was to facilitate discussions and obtain feedback regarding:

- The way in which roadside infrastructure would be established and the potential costs
- What lessons can be learned from the proposed European model

Discussions regarding roadside infrastructure highlighted the significant costs of roll out. Rolling out roadside infrastructure comes with a significant cost, one that most state and local agencies are not prepared or able to handle presently.

Additional take away points include:

- Some participants noted that each RSE installation could cost in the range of approximately $25,000 - $30,000. This rough estimate includes the cabinet, DSRC nodes, communications backhaul connections, and installation expenses.
- Participants also noted that the ability to leverage existing resources such as underground fiber varies from state to state based on factors such as usage limitations due to the original source of funding used to build or acquire the resources. Relief from such restrictions could potentially speed deployment.

The group also had deeper conversations about the European approach to rolling out connected vehicle systems, which provides a potential means of starting connected vehicle deployment to support mobility and other applications that do not involve imminent crash warnings. Key points brought up about this model, and suggested by stakeholders as considerations for USDOT, include:

- Use of OBEs with preloaded two year certificates placed on vehicles. At the end of two years, an alternative security solution would need to be in place for benefits to continue.

- Early services are focused on mobility messages, such as road conditions warnings, rather than hard safety warnings. Over time, if a stronger security model is created, then other safety and mobility messages could potentially be introduced.
- Most European countries have relatively restrictive privacy laws that govern the collection and management of PII within the proposed system.

Day 2 Breakout Session: System Ownership

The objective of the system ownership breakout session was for participants to discuss different ideas about how system ownership could work, with a particular focus on public-private partnerships (PPPs). The facilitator noted that the meaning of "public-private partnership" in this context was a joint ownership structure, not something that is owned and funded by the government with contracted involvement from the private sector. Participants were asked about successful PPPs with which they were familiar. Although some stakeholders felt that PPPs are discussed more often than they are implemented, individuals discussed different examples[2] including:

- No cost arrangements with state agencies – federal government provides oversight and guidance on activities, research, or goals of a project while state governments execute on operations, projects, and measurement of goals.
- Utility models that involve monopolies –utility companies that benefit from federal protection and/or subsidies to ensure monopoly or oligopoly operations.
- Shared agreements between state agencies and private telecommunication companies involving fiber optic lines – a representative from one state agency described an arrangement whereby the state and commercial organizations share rights, access, and revenue from fiber optic lines that benefits both parties for communications needs. Several other stakeholders mentioned similar arrangements with which they were familiar.

An important takeaway from this discussion was that leadership is key to the success of PPPs. PPPs that are led by large committees without specific assignments of responsibilities are likely to fall short of meeting their intended purpose. A clear understanding of how the different parties involved will benefit is also important.

The idea of a "public-public-private partnership" was also proposed. This idea would entail the USDOT partnering with another public agency as well as private agencies. A few key points from this discussion include:

- Because traffic congestion management applications have the potential to reduce emissions levels in addition to the obvious mobility benefits, it was suggested that the Department of Energy be considered as a possible partner, at least for certain aspects of the system.
- It was also suggested that the United Stated Postal Service (USPS) be considered as a potential system operator, in light of the fact that it is already a trusted entity and is in the process of transitioning to a more digital system for its own operations.

[2] Note that these examples reflect what participants spoke about during the workshop and have not been researched to provide actual names or legal arrangements in effect

Additional discussion involved the relationships between states and the federal government. Many participants expressed the need to have these relationships be more clearly defined in the context of the connected vehicle system. Of note:

- Stakeholders emphasized the differences among the states, and how regulations differ from locality to locality.
- Participants are seeking a clearer definition of the federal-state relationship to avoid a situation where multiple types of incompatible OBE or other technologies in the system are deployed across different states.

The breakout session closed with a discussion of privacy concerns related to system ownership. It was recognized that individuals are generally more comfortable with a private firm having access to their sensitive information than the government. Stakeholders also asserted that privacy protection is a context sensitive issue and that different instances dictate how and when an individual protects their information.

Day 2 Closing Prompt – A Question for All Participants

After the break out sessions, the workshop facilitators posed a question designed to collect direct feedback from participants on a range of actions that individuals and organizations could perform to support the development of the connected vehicle system. Participants were presented with the following question:

If you were CEO of your organization or an organization in your industry, what would you do to enable deployment and operation of a connected vehicle system?

Some of the responses to this question include the following:

- Roll out a popular application as soon as possible to get users into the system.
- Outfit a fleet of commercial vehicles as connected vehicles in a dense urban area and show off the benefits of the system.
- Provide the pole or power that will support DSRC installation in local/state governments.
- Offer non-monetary resources, such as land-use rights.
- Provide training for traffic professionals and technicians (via Institute of Transportation Engineers (ITE), unions, etc.) in order to get acceptance from traffic jurisdictions, particularly smaller cities.
- Adopt the European approach to deployment by OEMs: consider different approaches to privacy protection and urge the federal government to codify use of the data from the system to mitigate complexity and cost of the communications security infrastructure.
- Explain how the benefits of the system outweigh the costs; develop a set of standards to create a seamless environment across states; and identify funding sources to help with deploying, operating, and maintain the system.
- Clarify the roles for infrastructure, owner/operators, auto manufacturers, communications providers, USDOT, etc.

- Invest in Traffic Management Center capability that can take traffic data from DSRC and other sources and generate per-lane, even per-car, speed advisories.

Appendix A. Workshop Agenda

Public Workshop: Enabling a Secure Environment for Vehicle-to-Vehicle and Vehicle-to-Infrastructure Transactions
April 19 – 20, 2012

Meeting Objectives

- Update stakeholders on policy work for the connected vehicle research program.
- Update stakeholders on analysis performed to date to identify options to support communications security needs, including back end processes and alternative network options.
- Solicit input from stakeholders on critical areas of analysis, including business models and operational considerations.
- Provide opportunities for stakeholders to articulate concerns and challenges for anticipated implementation.

Thursday, April 19th

Presiding: Valerie Briggs, Team Lead, Knowledge Transfer and Policy, ITS Joint Program Office, Research and Innovative Technology Administration (RITA)

8:30am – 9:30am – Welcome and Connected Vehicle Policy Program Overview

- Welcome – Gregory D. Winfree, Deputy Administrator, RITA
- Connected Vehicle Program and Policy Research Overview – Valerie Briggs
- Legal/Policy Issues – Dana Sade, Legal Counsel, National Highway Traffic Safety Administration (NHTSA)
- Infrastructure Perspective – Robert Arnold, Director, Office of Transportation Management, Office of Operations, Federal Highway Administration

9:30am – 10:30am – Security System Analysis – Overview of Research and Interim Findings

- Security Approach Developed by the Auto Industry and Security Experts – Tom Schaffnit, Honda R&D, and President, Vehicle Infrastructure Integration Consortium
- Certificate Management Entities (CME) Organizational and Institutional Analysis – Dominie Garcia, Booz Allen Hamilton
- Communications Data Delivery Systems (CDDS) Analysis – Jim Misener, Booz Allen Hamilton

10:30am – 10:45am – Break

10:45am – 12:00pm – Connected Vehicle Applications and Stakeholder Needs

- Data Needs and the Basic Safety Message – Brian Cronin, ITS JPO, RITA
- Core System Stakeholder Analysis – Volker Fessman, Federal Highway Administration
- AASHTO Connected Vehicle Infrastructure Deployment Analysis – Jim Wright, American Association of State Highway and Transportation Officials

12:00pm – 1:15pm – Lunch

1:15pm – 2:45pm – Breakouts

- Business Model Framework Considerations
- Operational and Implementation Considerations

2:45pm – 3:00pm – Break

3:00pm – 4:30pm – Breakouts

- Business Model Framework considerations
- Operational and Implementation considerations

4:30pm – 5:00pm – Day One Wrap Up

Friday, April 20th

8:30am – 9:15am – Outcomes of Day 1 Breakout session

9:30am – 10:45am – Breakout Follow Up – Flexible to discuss outstanding issues and stakeholder driven requests related to previous day's work

10:45am – 11:00am – Break

11:00am – 12:30pm – Wrap Up and Next Steps

- DOT – Valerie Briggs
- CME – Dominie Garcia
- CDDS – Jim Misener

12:30 – Adjourn

Appendix B. Acronym Dictionary

API	Application Program Interface
BSMs	Basic Safety Messages
BW	Bandwidth
CA	Certificate Authority
CA_{ACT}	Certificate Authority Activation
CDDS	Communications Data Delivery System
CICAS	Cooperative Intersection Collision Avoidance Systems
CMEs	Certificate Management Entities
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DMA	Dynamic Mobility Applications
DSRC/WAVE	Dedicated Short Range Communications/Wireless Access in Vehicular Environments
ECC	Elliptic Curve Cryptography
HSM	Hardware Security Module
LA	Linkage Authority
LAN	Local Area Network
MDM	Misbehavior Detection and Management
OBE	On Board Equipment
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
RA	Registration Authority
RA_{ACT}	Registration Authority Activation
RFI	Radio Frequency Interface
RFID	Radio Frequency Identification
RSE	Roadside Equipment
SDARS	Satellite Digital Audio Radio Service
SPaT	Signal Phase and Timing
V2I	Vehicle-to-Infrastructure
V2V	Vehicle-to-Vehicle
V2X	Vehicle-to-Device
VII	Vehicle Infrastructure Integration
VIN	Vehicle Identification Number
WAN	Wide Area Network
WAP	Wireless Application Protocol
WiMax	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WWAN	Wireless Wide Area Network

Appendix C. References

United States. Department of Transportation. Intelligent Transportation Systems Joint Program Office. USDOT Announces Public Meeting on Enabling a Secure Environment for Vehicle-to-Vehicle and Vehicle-to-Infrastructure Transactions,' http://www.its.dot.gov/meetings/v2v_meeting.htm (May 2012).

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

U.S. Department of Transportation

Research and Innovative Technology Administration