RITA Research and Innovative Technology Administration

Intelligent Transportation Systems (ITS) Policy Program: Safety Policy Review and Discussion

August 3, 2011

Valerie Briggs
Team Lead
Knowledge Transfer and Policy
Research and Innovative Technology Administration
U.S. Department of Transportation

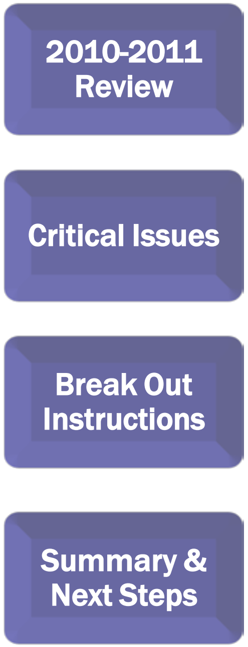
Presentation Topics

1. 2010-2011 Safety Policy Review
   - □ Policy Program in Support to V2V/V2I Program
   - □ Roadmaps
   - □ Accomplishments since last workshop (August 2010)
   - □ Stakeholder Engagement

2. Discussion
   - □ Governance
   - □ Approach to Communications Security/Security Infrastructure

3. Break Out Session Instructions

4. Key Takeaways, Summary, and Next Steps



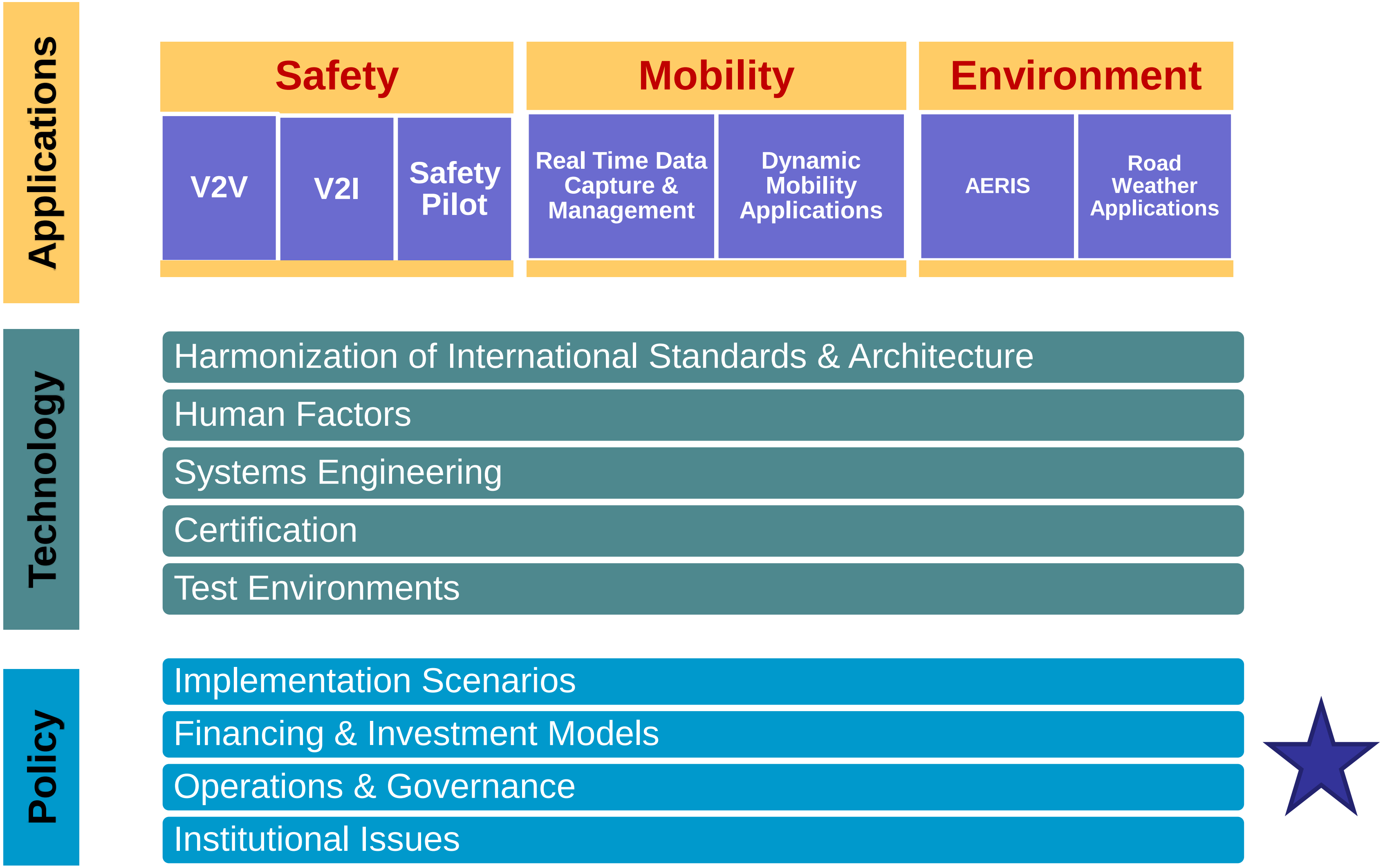
2010-2011 Review

Critical Issues

Break Out Instructions

Summary & Next Steps

The Policy Program:
Support of the Connected Vehicle Research Program



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

- Implementation Scenarios
- Financing & Investment Models
- Operations & Governance
- Institutional Issues

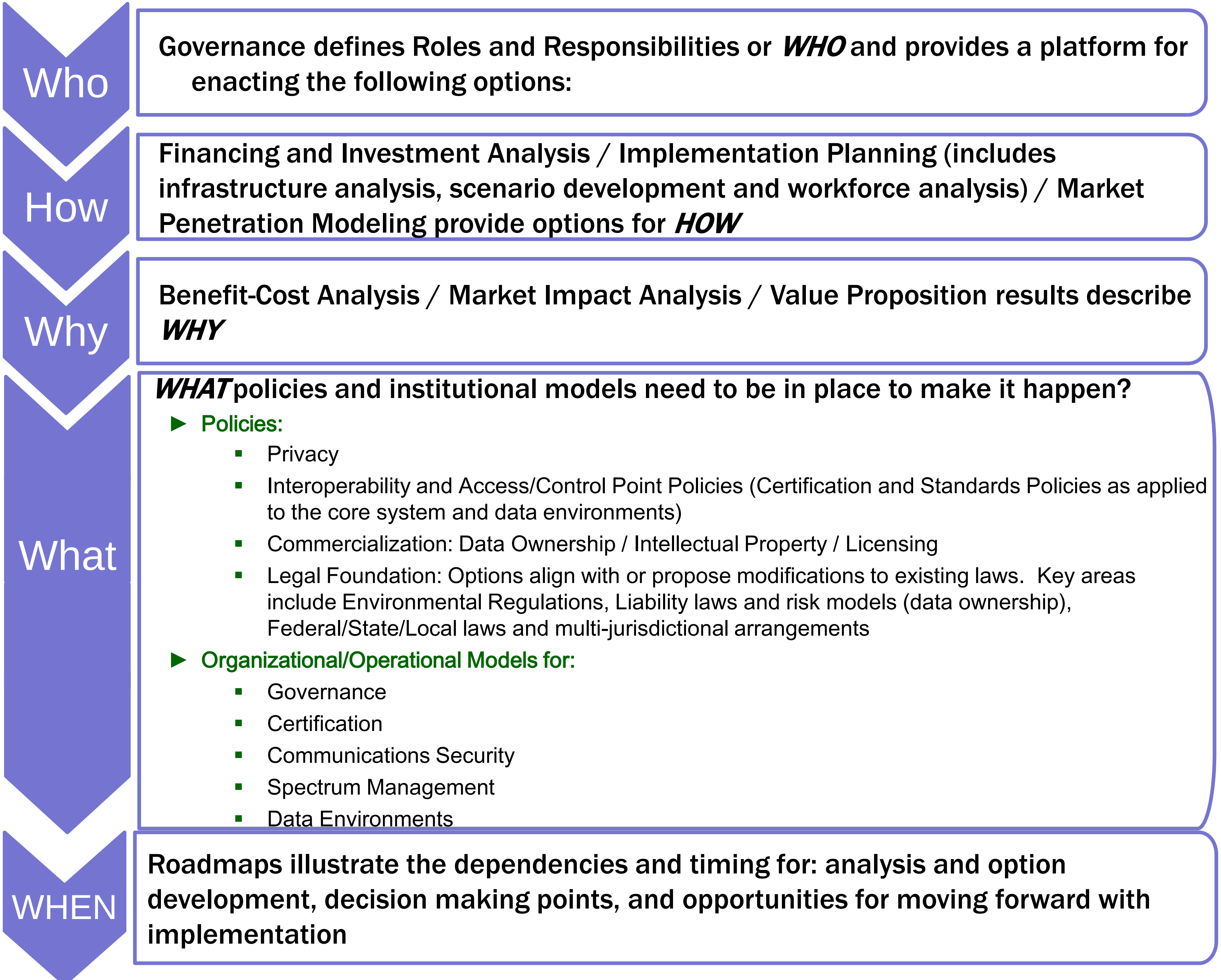
Identified Challenges

Global, Cross-Cutting Policy Issues

- **Governance**
- **Financing and Investment**
- **Institutional Issues:**
  - Privacy
  - Risk and Liability
  - Data Ownership
- **Benefit-Cost Analysis**
- **Implementation Planning**
- **Market Impact and Barriers to Adoption**

Technical Policy Issues

- **Safety Policy (options needed for support of NHTSA Agency Decision):**
  - Communications Security
  - Interoperability: Policies on Certification/ Interface & Access Points/ Standards
  - Spectrum
- **Mobility Policy:**
  - Data Governance
  - Intellectual Property and Licensing
  - Open Source / Procurement Strategies
- **AERIS Policy:**
  - Environmental Regulatory Structure (CAFÉ, Carbon Reduction, Cap & Trade, etc.)
- **Truck & Transit Policy**
  - Value Propositions
  - Retrofit Issues
  - Migration from other forms of communications media



Who

Governance defines Roles and Responsibilities or *WHO* and provides a platform for enacting the following options:

How

Financing and Investment Analysis / Implementation Planning (includes infrastructure analysis, scenario development and workforce analysis) / Market Penetration Modeling provide options for *HOW*

Why

Benefit-Cost Analysis / Market Impact Analysis / Value Proposition results describe *WHY*

What

***WHAT* policies and institutional models need to be in place to make it happen?**

- Policies:
  - Privacy
  - Interoperability and Access/Control Point Policies (Certification and Standards Policies as applied to the core system and data environments)
  - Commercialization: Data Ownership / Intellectual Property / Licensing
  - Legal Foundation: Options align with or propose modifications to existing laws. Key areas include Environmental Regulations, Liability laws and risk models (data ownership), Federal/State/Local laws and multi-jurisdictional arrangements
- Organizational/Operational Models for:
  - Governance
  - Certification
  - Communications Security
  - Spectrum Management
  - Data Environments

WHEN

Roadmaps illustrate the dependencies and timing for: analysis and option development, decision making points, and opportunities for moving forward with implementation

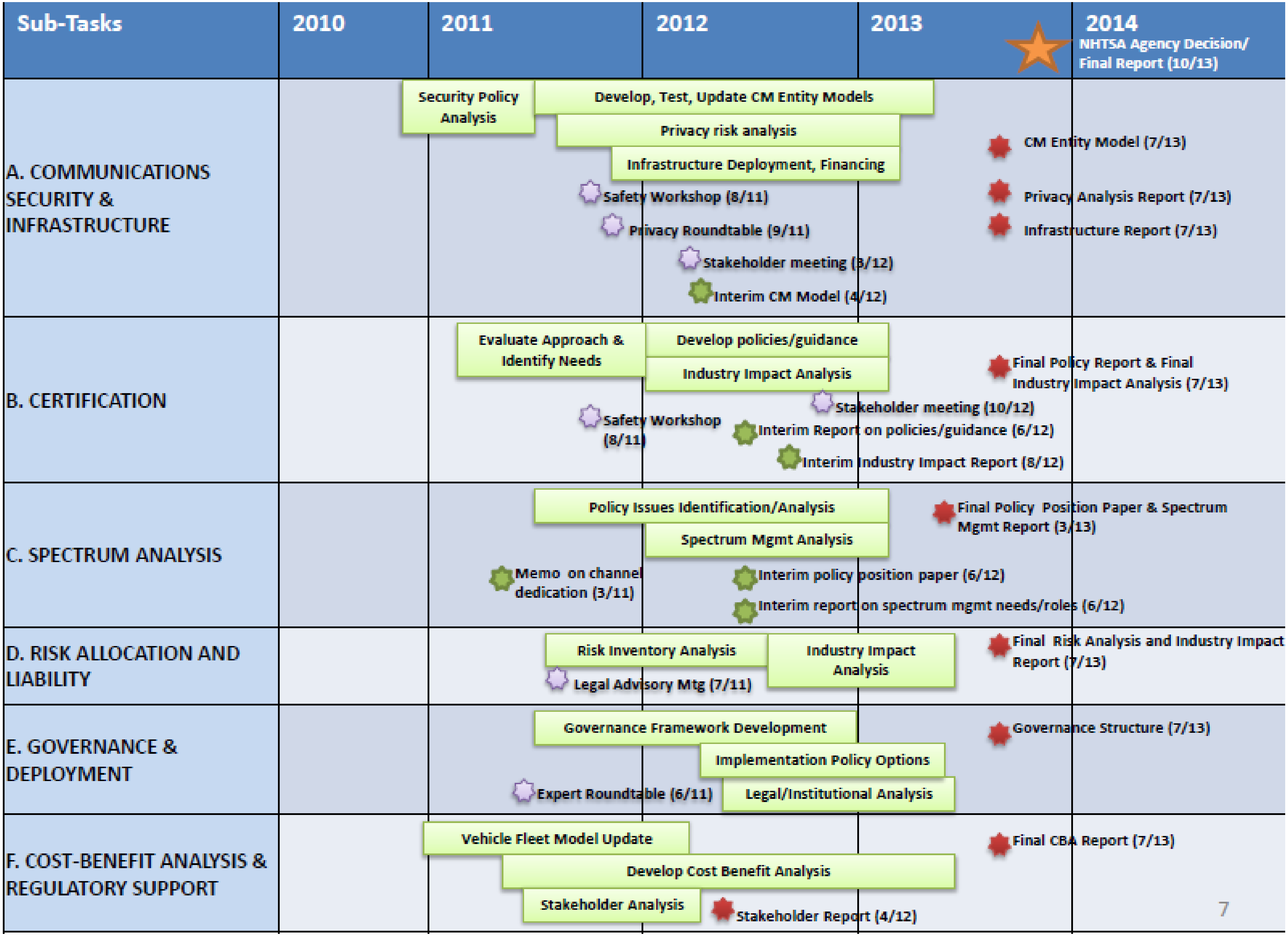
Where Are We Now? Roadmaps

- **Developed roadmaps:**
  - Global, cross-cutting roadmap
    - New version now available based on common issues between safety and mobility
  - Safety Policy Roadmap
    - Well vetted through Safety team and stakeholders
    - Key activities in support of NHTSA 2013-2014 agency decision have been prioritized
- **Roadmaps under development:**
  - Truck policy roadmap
    - Draft roadmap vetted with trucking stakeholders
    - Focus is on value propositions
  - Mobility policy roadmap
    - Draft Roadmap under internal review.
  - AERIS policy roadmap
    - Working draft
    - Focus is on crosscutting issues (across the TCs)
  - Transit policy roadmap
    - Under development

Global Policy Roadmap

Sub-Tasks	2010	2011	2012	2013	2014
A. Foundational Activities: Issues Identification, Roadmaps, and Execution Plans	Safety Workshop (7/10)	Safety Policy Roadmap & Execution Plan AERIS, Mobility & Truck Policy Roadmaps & Execution Plans Transit Policy Roadmap & Execution Plan Truck Policy Webinar Safety Workshop (8/11)		NHTSA Agency Decision/ Final Report (10/13)	FHWA and FTA Guidance Decisions FMCSA Review
B. Governance Development (overlaps with Safety Policy Roadmap)		Governance Framework Development Mapping of Govn. Space Expert Roundtable (6/11)	Governance Options Implementation Options Legal/Institutional Analysis Expert Roundtable (1/12)	Governance Structure (7/13)	
C. Investment/Financing Strategies	White Paper on Options (10/10) Market Penetration Model	Review of Arch./ID opportunities	Financial Modeling & Update to Market Penetration Model Options/Stakeholder meeting (12/12)	Final Investment/Financing Options (10/13)	
D. Core System Policies and Interface & Access/Control Points Framework		Analysis of Risk/Interfaces Policy Framework Devlpmt Devlpmt of System Metrics	Draft Framework (6/12)→ Feeds Organizational Models for Certification and Security; Metrics feed into Governance Models; Access Policies impact Data Environments & Applications Options/Stakeholder meeting (9/12)		
E. Cost-Benefit Analysis/ Value Propositions	Fleet Model Update Retrofit Analysis	Truck/Transit Value Props ASD Market Analysis	NHTSA Analysis (Cost-Effective, Benefits, etc. / FHWA/FTA Policy Analysis (?)	Final BCA (10/13)	
F. Deployment Planning and Systemwide Rules of Operation	AASHTO Deployment Planning	Prototype System Rules of Operation	Workforce Impact Analysis and Developmt of Guidance & Training	Delivery of Guidance and Training (12/13)	
G. Outreach	Workshops, Webinars, Reports,				

V2V/V2I Safety Policy Roadmap



Sub-Tasks | 2010 | 2011 | 2012 | 2013 | 2014

NHTSA Agency Decision/ Final Report (10/13)

A. COMMUNICATIONS SECURITY & INFRASTRUCTURE

Security Policy Analysis

Develop, Test, Update CM Entity Models

Privacy risk analysis

Infrastructure Deployment, Financing

Safety Workshop (8/11)

Privacy Roundtable (9/11)

Stakeholder meeting (3/12)

Interim CM Model (4/12)

CM Entity Model (7/13)

Privacy Analysis Report (7/13)

Infrastructure Report (7/13)

B. CERTIFICATION

Evaluate Approach & Identify Needs

Develop policies/guidance

Industry Impact Analysis

Safety Workshop (8/11)

Stakeholder meeting (10/12)

Interim Report on policies/guidance (6/12)

Interim Industry Impact Report (8/12)

Final Policy Report & Final Industry Impact Analysis (7/13)

C. SPECTRUM ANALYSIS

Policy Issues Identification/Analysis

Spectrum Mgmt Analysis

Memo on channel dedication (3/11)

Interim policy position paper (6/12)

Interim report on spectrum mgmt needs/roles (6/12)

Final Policy Position Paper & Spectrum Mgmt Report (3/13)

D. RISK ALLOCATION AND LIABILITY

Risk Inventory Analysis

Industry Impact Analysis

Legal Advisory Mtg (7/11)

Final Risk Analysis and Industry Impact Report (7/13)

E. GOVERNANCE & DEPLOYMENT

Governance Framework Development

Implementation Policy Options

Legal/Institutional Analysis

Expert Roundtable (6/11)

Governance Structure (7/13)

F. COST-BENEFIT ANALYSIS & REGULATORY SUPPORT

Vehicle Fleet Model Update

Develop Cost Benefit Analysis

Stakeholder Analysis

Stakeholder Report (4/12)

Final CBA Report (7/13)

Safety Policy Roadmap: Communications Security & Infrastructure

- **Objective:** Develop the institutional options in support of a technical communications security solution.
- **Steps/Milestones:**
  - **Develop Certificate Management Organizational/Operational Models:**
    - Options due in winter 2011
    - Approach for Safety Pilot testing: March 2012
    - Test Results and Evaluation of Approach: August 2013
    - Final Report: October 2013
  - **Analyze Infrastructure Options:**
    - Requirements Definition: Fall 2011
    - Analysis of Communications Options: Winter 2011/12
    - Implementation Requirements and Business Models: Spring 2012
- **Progress/Accomplishments:**
  - Analyzed technical approach and identified policy issues and trade-offs
  - Chose DSRC for Safety Pilot

Safety Policy Roadmap: Certification

- **Objective:** Develop the institutional options that assure interoperability.
- **Steps/Milestones:**
  - **Policy Framework /Policies on interface access/control points:**
    - Draft a policy framework that identifies Core System interface points for certification/standards: Winter 2011/2012
    - Finalize policy framework: October 2013
  - **Develop/Analyze Institutional Models and Market Impacts:**
    - Using technical process/metrics (beginning 2012), define institutional model options, including draft policies in support of technical process: Summer 2012
    - Analyze market impacts: Fall 2012
    - Final recommendation: October 2013
- **Progress/Accomplishments:**
  - Analyzing policy issues with core system
  - Reviewing technical certification process
  - Planning for development of policy framework

Safety Policy Roadmap: Spectrum Analysis

- **Objective:** Establish policies to transition the Dedicated Short Range Communications (DSRC) 5.9 GHz spectrum from research use to commercial use.
- **Steps/Milestones:**
  - **Needs Analysis for Spectrum Management:**
    - Identify potential need and institutional processes for spectrum management: Spring 2012
  - **Ongoing Communications with NTIA and FCC as Needed**
    - present – October 2013
- **Progress/Accomplishments:**
  - Met with FCC in Fall 2010 to provide program update
  - Met with FCC in April 2011 to clarify use of channels based on test results

Safety Policy Roadmap: Governance

- **Objective:** Develop a governance framework and policy options to support national implementation
- **Steps/Milestones:**
  - **Develop Governance Options:**
    - Engage experts to identify analytical path and lessons learned from other industries: June 2011
    - Understand needs: August 2011 (this workshop)
    - Develop and evaluate options (test during Safety Pilot): Summer 2012
    - Aggregate results of all policy efforts related to Governance models and final report: Summer/Fall 2013
    - Identify implementation needs: Fall 2013
  - **Analyze Challenges:**
    - Analyze State/Local laws, multi-jurisdictional issues, and other potential challenges to implementation: Summer 2013
    - Identify and develop guidance in support of implementation: Summer 2013
- **Progress/Accomplishments:**
  - Held Governance Roundtable with experts: June 2011

Safety Policy Roadmap: Risk/Liability

- **Objective:** Address relevant legal issues
- **Steps/Milestones:**
  - **Identify new risks and legal issues:**
    - Scope issues / develop risk inventory: now – Spring 2012
    - Conduct research and develop options for mitigation/new policies/policy modifications: Spring 2013
    - Final report on potential mitigation strategies: October 2013
- **Progress/Accomplishments:**
  - Have identified legal issues and will be working with a DOT legal task force to scope policy research plan

Safety Policy Roadmap: Cost-Benefit Analysis and Regulatory Support

- **Objective:** Develop comprehensive analysis of total benefits and costs of implementing a connected vehicle environment. Develop a rigorous benefits-cost framework for making a NHTSA agency decision.
- **Steps/Milestones:**
  - **Vehicle Fleet Model/Market Penetration Analysis:**
    - Update fleet model/ conduct market penetration analysis to estimate adoption rates: now – Summer 2013
  - **Value Propositions:**
    - Identify the direct financial impacts for different stakeholder/industry groups (e.g. OEMs, State and local transportation agencies, transit agencies, trucking companies): now – Summer 2012
  - **Impact Analysis**
    - Using Safety Pilot results , cost models, value propositions, conduct an analysis on the economic and societal impact of a NHTSA agency decision: starts October 2013
- **Progress/Accomplishments:**
  - Updated fleet model, developed cost estimate of retrofit option, and in process of assessing aftermarket device options.
  - Developed framework for value propositions: Starting truck and transit, NCHRP study for State and local agencies.

Policy Alignment with Technical Programs

- **Core System:** Aligning policy needs with Core System based on ConOps and System Requirements (waiting on Architecture to define Interface Policy Framework)
- **Standards:** Working with Standards Program to support international harmonization efforts and identify how Standards are tools that support policies
- **Certification:** Working with Certification team to develop institutional models and identify market impacts/requirements
- **Communications Security:** Developed policy analysis for Communications Security (see white paper) as basis for additional analysis
- **Open Source Portal Policies:** Assessing governance and licensing issues with open source approach; and operational models
- **Dynamic Mobility Applications Policy Issues:** Conducted initial analysis on risks, data sensitivities, and market issues
- **Truck Policy:** Hosted webinar on truck policy
- **Implementation Scenarios:** AASHTO completed its scenarios report and presented findings

Additional Activities, 2010-2011

- **V2V/V2I Senior Policy Task Force:**
  - Internal multi-modal executive working group in DOT
  - Formed in March 2011, meets regularly
- **Stakeholder Engagement:**
  - Implementation scenarios workshop–June 2010
  - Safety workshop–July 2010
  - Mobility workshop—December 2010
  - Truck Policy webinar—February 2011
  - Governance roundtable –June 2011
  - Safety workshop – August 2011

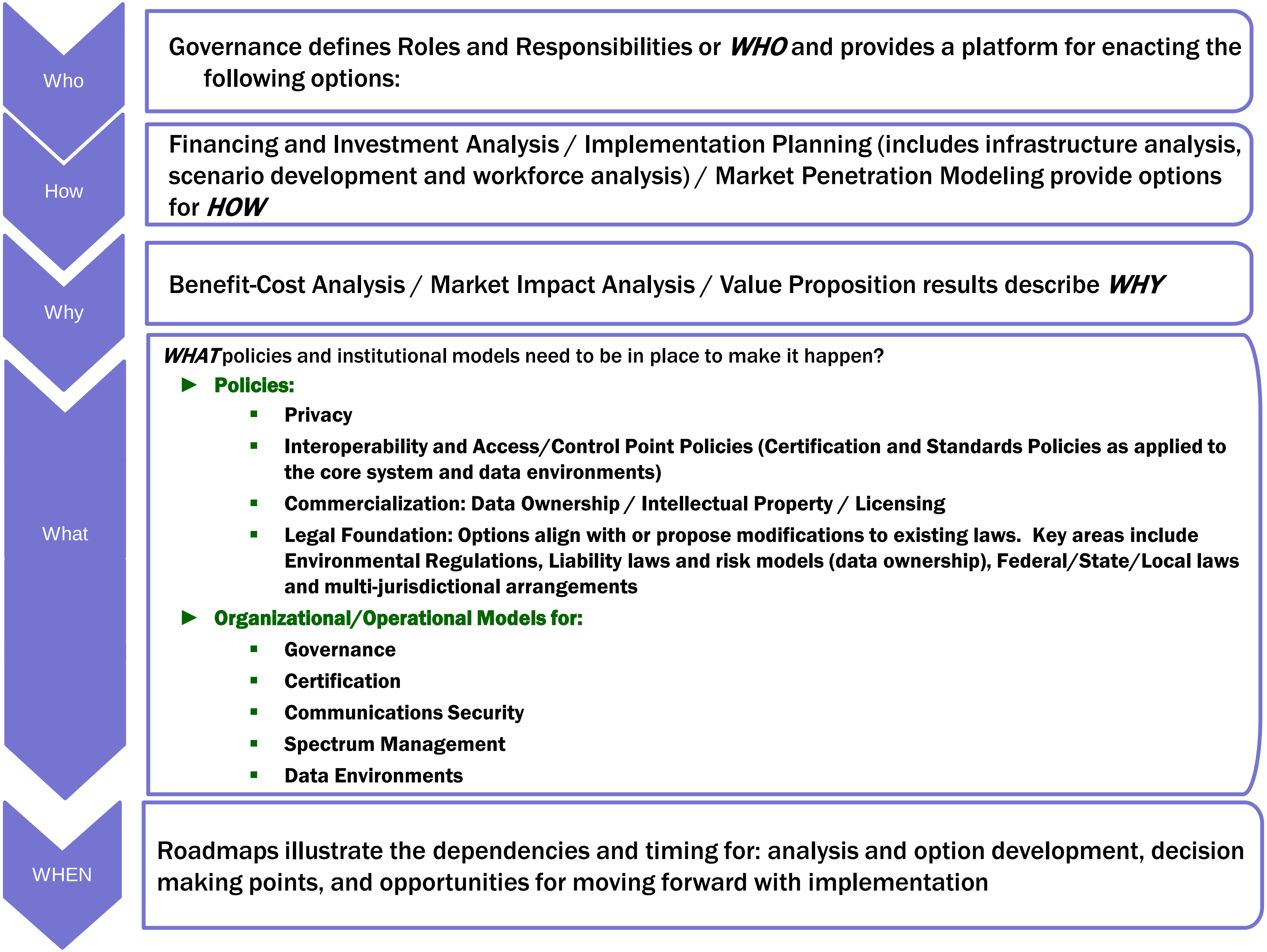
Today's Discussions

1. Governance – Terry Regan, US DOT/Volpe Center, Presenter
   - Review expert knowledge about how to structure Governance and lessons learned from other industries
   - Gather stakeholder input in break-out sessions

2. Approach to Communications Security and Security Infrastructure – Suzanne Sloan, US DOT/Volpe Center, Presenter
   - Review approach developed using expert input
   - Discuss options for turning approach into prototype for testing
   - Discuss next steps

Governance

Review: Role of Governance



Who

Governance defines Roles and Responsibilities or ***WHO*** and provides a platform for enacting the following options:

How

Financing and Investment Analysis / Implementation Planning (includes infrastructure analysis, scenario development and workforce analysis) / Market Penetration Modeling provide options for ***HOW***

Why

Benefit-Cost Analysis / Market Impact Analysis / Value Proposition results describe ***WHY***

What

WHAT policies and institutional models need to be in place to make it happen?

- **Policies:**
  - **Privacy**
  - **Interoperability and Access/Control Point Policies (Certification and Standards Policies as applied to the core system and data environments)**
  - **Commercialization: Data Ownership / Intellectual Property / Licensing**
  - **Legal Foundation: Options align with or propose modifications to existing laws. Key areas include Environmental Regulations, Liability laws and risk models (data ownership), Federal/State/Local laws and multi-jurisdictional arrangements**
- **Organizational/Operational Models for:**
  - **Governance**
  - **Certification**
  - **Communications Security**
  - **Spectrum Management**
  - **Data Environments**

WHEN

Roadmaps illustrate the dependencies and timing for: analysis and option development, decision making points, and opportunities for moving forward with implementation

Relevant Industry Governance Models

- **Healthcare Industry / Health IT –** Framework for policy and technology practices while protecting privacy; offers insights into standards setting, governance
- **Public Safety / Emergency Response Communications** – Highlights the issue of interoperability as well as issues dealing with spectrum sharing.
- **National Standards of Standards and Technology (NIST) –** Provides government-wide examples of challenges with technology adoption and insights into analysis of private sector and the cost/value proposition.
- **Internet / ICANN (Internet Corporation for Assigned Names and Numbers)** – Provides an example of governance structures already being in place (implemented by the US Department of Commerce) but then dismantled and reconstructed to transition management to the global community.
- **Smart Grid –** Highlights how governance issues related to consumer data, security issues and data ownership can have innovation implications.
- **Telecommunications / Cell phone industry:** The governance of the cell phone industry is relevant as a parallel to a transportation communications system.
- **Cognitive radio –** Example of governance structure that used to be a federal government function, but is now in a private sector laboratory which has been delegated a government role. Also deals with issues concerning wireless governance, spectrum sharing and white space.

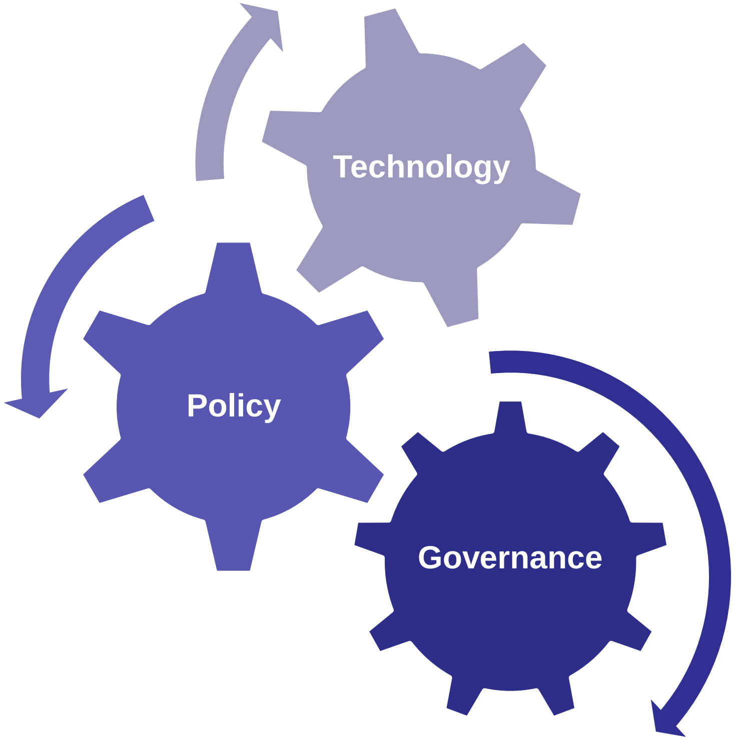
Best Practices: Stakeholder Involvement

√ Multi-stakeholder engagement is critical.

- Identify “veto or dispute points” early in the process.
- Make use of the innovative techniques/technologies for engaging the public and give voice to a wide range of groups during the governance-setting process.
- Consider horizontal and vertical perspective when evaluating stakeholder impacts:
  - Horizontal–inter-agency ties within one level of government.
  - Vertical–different levels of government, for example, between state and local. Typically, local and state entities are responsible for implementation, which could have a large effect on governance.

Best Practices: Developing Governance

- √ Develop technology and policy simultaneously as technical decisions tend to have social and economic implications.
- Develop Governance in concert with policy—they should not be separate program tracks.
- Map the intersection between governance and information, specifically the role of information ownership.
- Consider implications for innovation and competition and how they impact/influence the options for governance structure.



Best Practices: Privacy

- √ Implement “privacy by design” early in the process—note that all information can or should not have to be treated equally.
- √ Note that privacy is more than anonymity—it is also a set of clear, transparent, enforceable principles for how data will be collected, used, accessed, and/or stored.
- √ **Fair Information Practice Principles (FIPPs):** A solid example of how to best deal with information from both a privacy and information management perspective. FIPPs is a process for identifying the purpose of information collection and to determine if the correct information is being collected.
  - Good examples include: Department of Homeland Security (DHS), Health and Human Services (HHS), and the Organization for Economic Cooperation and Development (OECD).

✪ The 2007 Privacy Principles for VII were based on the OECD principles.

Developing Governance

- *We asked the experts:* "What does the program need to do to define a governance structure for new technologies/systems?"

- The response was 3 steps:
  - □ **Step 1: Define Why Governance is Needed/Who is Involved**
    - Define Mission and Goals
    - Define Good Governance Principles, based on the Mission
    - Identify Trade-offs and Downstream disputes
  - □ **Step 2: Map Governance –**
    - **Who else has defined governance/authority in this space?**
    - **What is the legal landscape in this space?**
  - □ **Step 3: Develop Governance Options**
    - Develop Approach(es)
    - Develop a Policy Framework for use of Tools such as rules, standards, certification, etc.
    - Develop Privacy Strategy – turn principles into policy/design

Step 1: Determine Mission and Goals

- Determine a mission and goals for the program
- Establish appropriate good governance principles for the program. Examples include:
  - Participation / Voice – Those who will be impacted by the system will be part of the decision making process
  - Accountability – Clearly defined process for how to address disputes
  - Representation – Recognized stakeholder participation and interests
  - Transparency – Clarity on how and why decisions were made
  - Efficiency – Recognize that there are trade-offs with participation
  - Flexibility – Don’t lock into decisions that may lead to stalled innovation
- Evaluate and prioritize the list of defined principles and identify potential trade-offs
- Identify areas where market failures may impact the governance model – how much will failure be tolerated? Answer will help identify where the Federal government is needed most.
  - Note that the less tolerant of failure, the less tolerant of innovation and the more centralized control and limited access is required. Evaluating failure will determine levels of tolerance and drive the regulatory structure.

An Important Highlight

- Safety vs. Mobility/Environment–Experts noted that we have mission/goals that might be in some conflict with one another. They asked:
  - Is it about enhancing safety or improving mobility or mitigating environmental degradation? Or all?
  - It is about establishing trust and interoperability?
  - Others? Which are the priorities?
- They noted that there are potentially different roles for government in each:
  - A safety goal will require a different governance process and a different Federal role as opposed to goals for enabling mobility and environmental applications.
  - Goals will help to determine which stakeholders will be at the table.
  - Use of regulatory tools, standards, and other rules differ, but so does access and enforcement.
  - Privacy issues in safety seem to be far less of a privacy concern than for mobility.

Step 2: Map Governance

- Process of identifying what other agencies or organizations having existing governance structures or authority that might overlap with the V2V/V2I governance needs. Mapping describes both:
  - The current situation
  - The entities that coordinate governance versus the entities with the authority that are needed to enforce interagency coordination.

- Experts suggested mapping the following elements:
  - Stakeholders – who is central to the network and what relationships are present between stakeholders?
  - Roles of Federal, state, and local government
  - Roles of public institutions
  - Existing private sector involvement
  - Operational network – who is in charge of each particular aspect, who has authority to make decisions?
  - Budget categories and public spending trends

Step 3: Develop Governance Options

- Analyze strengths, weaknesses, and relevance of **different approaches** for meeting V2V/V2I needs:
  - *Holistic vs. Organic*:
    - Holistic: A total systems or systems engineering approach—May be valuable to inform the 2013 process and other processes
    - Organic: An evolutionary approach to incrementally implementing the system and running early on and learning by doing—Builds confidence with the things that work early on, a way of "growing" a system.
  - *Centralized vs. Decentralized*
  - *Hybrid*
  - *Others*
- Identify what **different types** of governances are needed for V2V/V2I. Governances typically exists at different levels:
  - Regulatory governance – involves typical decisions on price setting, anti-trust issues
  - Public policy governance & values – involves moral / social values, issues surrounding privacy
  - International governance – involves international affairs, national security and defense
  - Others
- Examine the **different processes or functions** of governance.
  - Functions help work towards certain goals, such as trust and interoperability. Mechanisms will need to be developed to perform each function.

Governance may be Governances!

It is possible to have many “governances” for the V2V/V2I system

Governance Tools and Lessons in Application

- Standards:
  - Do not ‘over-develop’ standards.
  - Consider the use of ‘soft law’ where standards are set and then benchmarking is established to determine if people are meeting benchmarks voluntarily.
- Regulation:
  - Look at the model of Rulemaking Workshops and Negotiated Regulations (RegNeg) in various case studies. RegNegs are used to identify critical issues, create consensus, or help mitigate disputes. The decisions are not binding on the agency or stakeholders. This has typically been used in the EPA and OSHA in developing industry standards.
- Certification:
  - Certification can be a great enforcement tool and establishes trust – an essential element in a cooperative safety system. Certification can have unintended consequences by locking in a certain type of technology and inhibiting innovation.
  - Certification represents an example where a wholly government function can be transitioned to the private sector. It is better to have multiple certifiers. This keeps standards high and encourages competition.

Governance Tools (continued)

- Enforcement:
  - Consider to what extent enforcement can be privatized if a public good (such as safety) is involved.
- Funding:
  - Funding can be a valuable and powerful governance tool depending on who is transferring funds and what the criteria is for funding transfers. This could affect the technology governance and help to understand what will prevail and how technology will be implemented.
- Consumer protection is important and the end user must be represented in the processes of governance.
- Information -governance frameworks identify important factors in protecting privacy:
  - For what purposes is the data or information collected?
  - When collected, is that enough data or information to deal with that purpose?
  - Collecting data that is not necessary? What is done with the collected data? Who has access? How long is it stored?
  - What if there is a change in the information being collected? Who is impacted? What are processes for facilitating the change?
  - How do you resolve disputes? Who is involved in the resolution? What are the remedies?

Key Lesson:

**Fully understand your governance tools and their potential cost implications as well as the consequences of not having them.

Recognize that there are costs even with self-governance.

Intent of Break-Out Sessions: Stakeholder Needs Analysis

Step 1: Define Why Governance is Needed/Who is Involved

- Define Mission and Goals
- Define Good Governance Principles, based on the Mission
- Identify Trade-offs and Downstream disputes

Step 2: Governance Mapping –

- Define who has established governance or authority
- Map the legal landscape

Step 3: Develop Governance Options

- Analyze Approach(es)
- Develop a Policy Framework for use of Tools such as rules, standards, certification, etc.
- Develop Options for Privacy

Today's Stakeholder Input:

- Revisit mission and goals, principles, trade-offs and potential disputes
- Assist with/Map governance interests
- Discuss approaches

Break — 10:45-11:00am

- **Next:**
  - Discussion of Communications Security
  - Instructions for Break Out Sessions

Communications Security – Approach

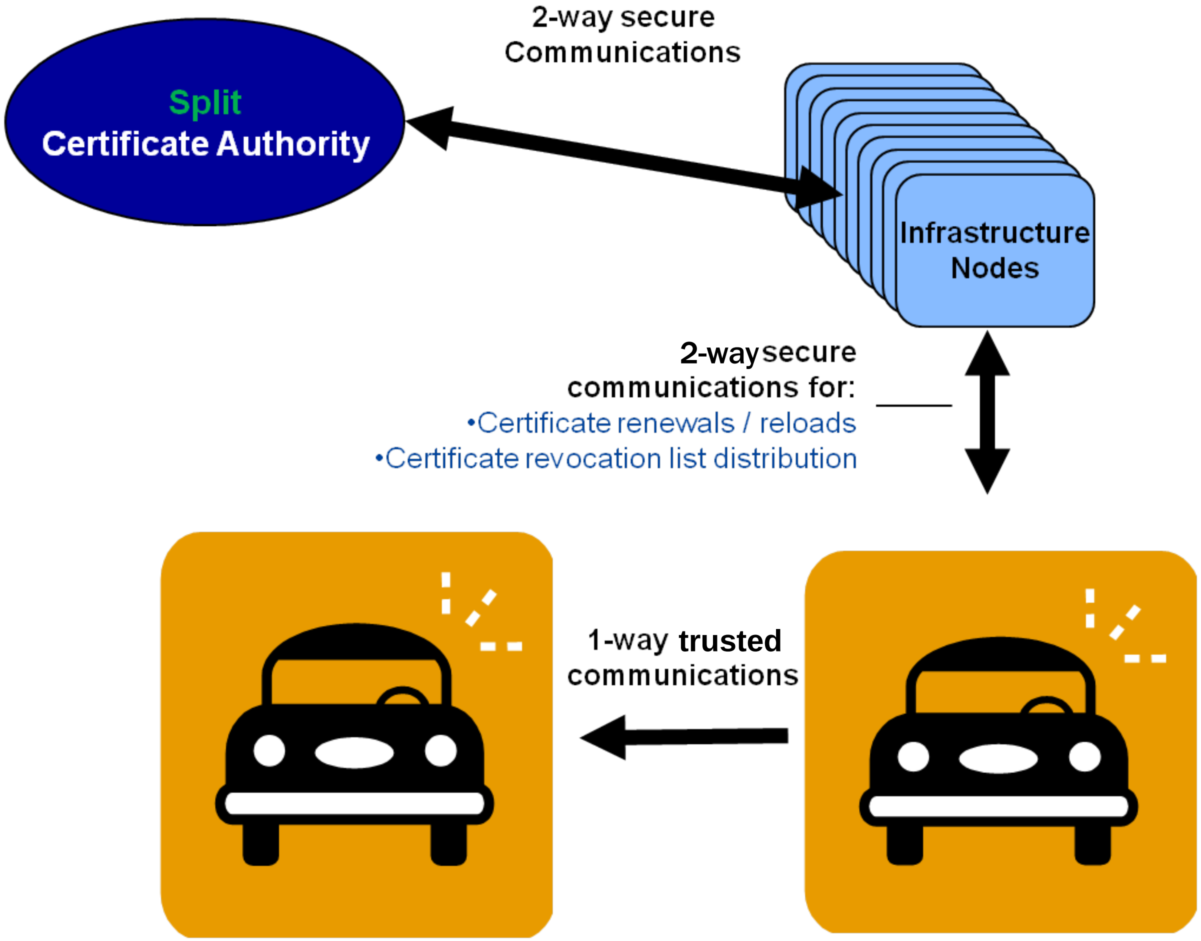
- Implementing V2V/V2I will require communications security
- Key part of the prototype system for which experts were engaged to develop an approach
- V2V/V2I has unique characteristics that differ from traditional systems. Major difference is that mission-critical systems typically do not use wireless. Key communications security requirements are:
  - **Provide trusted messages between vehicles** – trust is established through a user authentication process. These messages are not encrypted
  - **Secure messages between vehicles and certifying authority** – messages are encrypted to prevent eavesdropping and tampering over the communication channel
  - **Ensure Anonymity** - no personally identifiable information is contained in messages
  - **Allow for Scalability** – needed to support over 250 million vehicles in the system

Important Distinction in Development Path

- **Approach vs. Design vs. Model vs. System**
  - Approach = first step in identifying industry best practices and tailoring them to meet the requirements of a V2V/V2I environment for preventing, detecting, and mitigating security risks. Deliverable due in Fall of 2011.
  - Design = second step that structures the technical elements into a representative prototype. Deliverable due in Spring 2012.
  - Model = third step that combines the technical prototype with organizational and operational elements the results in a representative system to test and evaluate in real world environment. Deliverable due in Summer 2013.
  - System = last and final step is to combine test results with prototype model to understand the requirements/specifications for an operational system. Deliverable due in Fall 2013.

Description of Security Approach (continued)

Physical Configuration:


2-way secure Communications
Split
Certificate Authority
Infrastructure Nodes
2-way secure communications for:
•Certificate renewals / reloads
•Certificate revocation list distribution
1-way trusted communications

Description of Security Approach

- Three key elements:
  1. Public Key Infrastructure (PKI)
  2. Vehicle and other security elements
  3. Policies

1. PKI is an umbrella term used to describe the hardware, software, people, policies, and procedures needed to create, manage, store, distribute, and revoke digital certificates. For V2V/V2I, the PKI establishes trusted messages:
   - Provides authorization credentials to vehicles for participation in the network
   - Facilitates the revocation of credentials if an administrating authority decides to do so.
2. Vehicle and other security elements at the local (vehicle) level are incorporated to **prevent misbehavior** and **detect misbehavior already occurring** within the system. These include:
   - Hardware: standard controller on the vehicle + tamper-proof encasements
   - Software: functionality checks and misbehavior detection processes

Description of Security Approach (continued)

3. Policies, in combination with technical solutions, assist in preventing and addressing misbehavior. Such policies can include:
   - Legal deterrence for physical tampering with vehicle’s on-board equipment
   - User access policies
   - Split certificate management entity

Description of Security Approach (continued)

- Risks:
  - Analysis suggests minimal risk to safety in event of a successful attack.
  - Greatest risk appears to be in reducing acceptance (and use) of an operational system if users do not trust it and ignore it.
  - The identified privacy attacks would require a significant level of effort and investment to implement. Risk of these types of attacks is thus lower than utilizing existing methods for tracking (cell phone or physically following a vehicle).
  - The identified privacy or system attacks would require insider knowledge of the system or physical access to a vehicle.

Advantages and Limitations of the Approach

- **Advantages:**
  - Meets objectives of providing trusted, anonymous messages using random identifiers that are changed every five minutes
  - Is scalable to 250+ million users
  - Supports crash avoidance safety applications
  - Many attacks are only feasible with a significant amount of investment and expertise about the system
  - Approach prevents/mitigates against harm to the system

- **Limitations:**
  - No instantaneous identification of misbehaving actors; delay in identification and delay in removing misbehaving actors from system
  - Splitting the certificate management entity may have cost implications
  - Need frequent updates of certificates; as of now, our approach limits updates to driving by a roadside unit (RSE) as other options have significant challenges
  - Approach does not address system backhaul (RSE) connections

Technical - Policy Balance

- **Technical Requirements:**

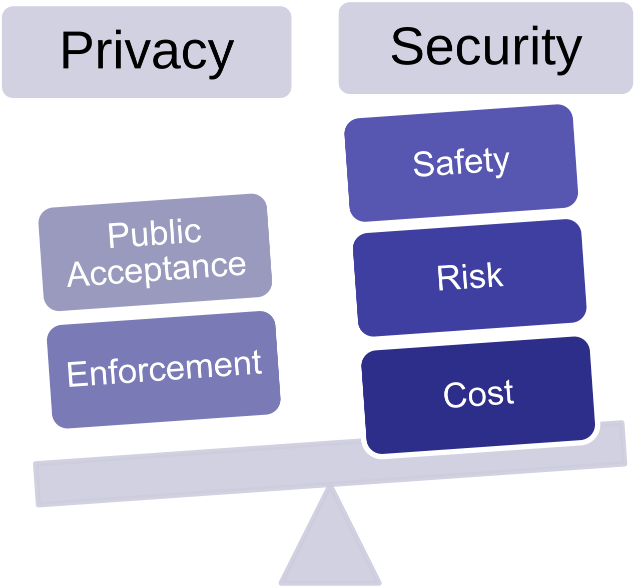
✓ Enable trusted communication between vehicles and secure communication between vehicles and the infrastructure

✓ Provide reasonable defense against attacks

✓ Protect privacy and personal information of users

✓ Reasonably balance privacy needs against security requirements

- **Balanced Approach:**
  - Privacy versus Safety versus Security
  - Safety versus Security
  - Security versus Cost



Example: Decision about Communications media

- Which communications media can support both the technical and the policy requirements? Viable choices include:
  - Existing Cellular Networks
  - Dedicated Short Range Communications (DSRC)
  - WiFi
- What are advantages and limitations of each?

- **Business Model Questions: –** *How much will it cost? Who will fund deployment, operations and maintenance? Ownership? Can commercial networks be used or leveraged? Can multiple networks be used or combined?*

Review of Options and Analysis to Date

Cellular Network
Advantages
Current privacy limitations are known and accepted through an opt-in option
Cellular infrastructure in place
In theory, meets the requirement to assure daily access to certificates
Limitations and Questions
Does not support privacy framework as it allows tracking and recording; can identify users
Usage is subscription-based
Lacks broadcast capabilities; existing networks would require enhancements–what are associated costs?
Vehicles using cellular for certificate management would also need DSRC for safety applications.

Analysis to Date:

- *Are there business models that would provide cellular service for certificate management without a subscription? Purchasing service in bulk? Who would be responsible for the purchase? Funding?*
- *What enhancements, if any, would be needed to use the existing cellular system for certificate management? Who will make the investment?*
- *Is reliability of the service an issue in terms of assuring that all vehicles receive their certificate updates?*
- *Are current cellular network security practices a risk in terms of illegally accessing certificates or associated information?*

Review of Options and Analysis to Date

5.9 GHz DSRC
Advantages
Meets the requirements for privacy and "anonymity by design"
Spectrum allocation gives greater control over access/rules of use
Full integration for V2V and V2I
DSRC network can be nationally scaled, works w/ high vehicle density
Limitations and Questions
No existing nationwide network—How much infrastructure is needed? Who owns, operates, and maintains?
High investment — How to fund implementation, operations, and maintenance? Private sector business models that support safety needs? How to enable consistent national approach if done privately or by jurisdiction?
Will need to have some sort of revenue stream or payment mechanism to support ongoing operations and maintenance.

Analysis to Date:

- *Methodologies to estimate amount of infrastructure needed in support of* ***V2V security*** *result in an estimate of approximate 40,000 RSEs to cover metropolitan areas (possibly nationwide footprint –further analysis is being pursued). May be able to leverage security infrastructure to support V2I applications, but will this be enough to provide V2I coverage and create benefits?*
- *This amount would support ability for near 100% of vehicles to receive certificates and revocation lists daily, thus minimizing security and safety risks.*

Review of Options and Analysis to Date

Wi-Fi
Advantages
Current privacy limitations known and accepted
Widely implemented and accessible
Commercial interests can support further implementation
Limitations and Questions
Does not support privacy framework
No coherent nationwide network
Coverage range is limited
Security is an issue
Allows tracking and recording

Analysis to Date:

- *WiFi may have some subscriptions fees.*
- *WiFi is high latency – does not easily support dynamic communications with moving vehicles.*
- *Is there a potential hybrid option?*

Next Steps for Communications Security

- Conclusion: Approach provides us with a solid basis for moving to next step– prototyping and analyzing business models.
- Next Steps:
  - Refine security approach
    - Interoperability and scalability tests Fall 2011
  - Engage privacy advocates
    - Privacy Roundtable – Outreach to privacy advocacy groups in Winter 2011
  - Identify options for organizational and operational scenarios (see Roadmap for Safety Policy)
    - Certificate Management Entities – Organizational and Operational Interim Models Spring 2012
    - Costs – Interim security cost estimates Spring 2012
    - Governance – Develop options and guidance for understanding roles and responsibilities – Spring 2012
  - Develop technical design (if appropriate) – Spring 2012
  - Test prototype during Safety Pilot Model Deployment

Questions?

Questions?

Break Out Session Instructions

- Four Rooms – Same session in each room
- Facilitator and Notetaker will be present; ask that the group appoint a representative to report out
    - San Francisco (Green): Facilitator is Suzanne Sloan; notetaker is Andrea Van Easton
    - New Orleans (Red): Facilitator is Terry Regan; notetaker is Jamie Weil
    - Hong Kong (Blue): Facilitator is Gary Ritter; notetaker is Julie Nixon
    - Regency A (Yellow): Facilitator is Valerie Briggs: notetaker is Kevin Gay

Intent of Break-Out Sessions: Stakeholder Needs Analysis

Step 1: Define Why Governance is Needed/Who is Involved

- Define Mission and Goals
- Define Good Governance Principles, based on the Mission
- Identify Trade-offs and Downstream disputes

Step 2: Governance Mapping –

- Define who has established governance or authority
- Map the legal landscape

Step 3: Develop Governance Options

- Analyze Approach(es)
- Develop a Policy Framework for use of Tools such as rules, standards, certification, etc.
- Develop Options for Privacy

Today's Stakeholder Input:

- Revisit mission and goals, principles, trade-offs and potential disputes
- Assist with/Map governance interests
- Discuss approaches

Summary

- Report Out from Groups
- Summary of what we heard
- Discussion of next steps