Policy Roadmap for IntelliDrive[SM] Safety: Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I)

DRAFT: 05/19/2010[1]

PURPOSE

The purpose of this paper is to describe a roadmap for conducting the policy research under the IntelliDrive[SM] Safety Program, a program focused on the technical research needed to develop, demonstrate, and test vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) technologies for safety.

The policy research will be prioritized and driven by the following:

- The 2013 NHTSA regulatory decision and the data and information needed to result in a fact-based and evidence-based policy decision.
- The five-year Safety Program roadmaps for addressing the V2V and the V2I technology issues.
- The Safety Pilot roadmap that describes an upcoming opportunity to test and create a model deployment for V2V and some limited V2I technologies under real-world conditions.

The Policy research is focused along two timelines:

- Those priority questions that need to be resolved to support the Safety Pilot and, ultimately, the NHTSA regulatory decision. These actions are needed in the near-term.
- Those questions and issues that need to be resolved in support of deployment of V2V and V2I for safety.

POLICY FOCUS AREAS

The following areas define the critical areas of focus for the IntelliDrive[SM] Safety Program Policy Roadmap. They include:

A. Device and Equipment Certification
B. Certificate Authority, Privacy, and Security
C. Risk Allocation and Liability / Data Ownership
D. Cost-Benefit Analyses in Support of NHTSA Regulatory Decision
E. Rules of Operation and Application of Standards
F. Spectrum Analysis and FCC Role
G. Infrastructure
H. Governance Structure and Authority (cross-jurisdictional, cross-vehicle model)

The remainder of this paper will describe each area and the policy issues, describe the actions and outcomes needed to support forward progress in IntelliDrive[SM] Safety, and present a roadmap for conducting the work.

[1] This document represents a first draft and requires further exploration and definition. This draft is intended to elicit comment and further inputs as a means of ensuring that this document becomes a comprehensive and well-defined roadmap for addressing policy issues related to V2V and V2I safety.

POLICY AREAS

A. DEVICE AND EQUIPMENT CERTIFICATION

Certification represents a key part of the IntelliDrive^{SM} system as it provides a process that ensures that all devices and equipment that connect with the IntelliDrive^{SM} system meet specific standards (criteria) relating to security, performance, and privacy.

Policy Questions

- What IntelliDrive^{SM} device and equipment need to be certified?
- What are potential IntelliDrive^{SM} device and equipment certification processes? What are the certification criteria (standards for security, performance, and privacy) against which devices and equipment will be tested?
- Who will develop the tests?
- Can aftermarket devices meet security requirements?
- Once designed, tested, and approved, what entity(ies) will oversee the process and provide certification? What is the role of the Federal government in ongoing certification, if any?
- Is any new authority needed to oversee IntelliDrive^{SM} device and equipment certification?
- Do existing certification laboratories for other industries provide any opportunities or lessons learned for IntelliDrive^{SM}?
- What are the institutional models for operating a device and certification process? Can this be a wholly private sector function?

Tasks

- Under the IntelliDrive^{SM} Systems Engineering Program, develop a certification process, certification criteria, and tests in collaboration with experts and stakeholders (manufacturers of vehicles, devices, and equipment).
- Review certification processes from other industries to identify lessons learned, opportunities, authorities needed, and role of the Federal government.
- Conduct a certification pilot study in early 2011 as part of the Safety Pilot.
- Based on lessons learned, modify the certification process.
- Identify steps for implementation. .
- Conduct stakeholder outreach, education, and collaboration throughout process. Key stakeholder groups identified below.
- Design guidance and/or training for agency procurement and maintenance personnel.

Stakeholder Collaboration:

The following stakeholders need to be considered as partners in developing or reviewing the process that is designed by experts:

- **Federal Government:** To be engaged in exploring certification processes, identifying needs and oversight. Stakeholders include ITS JPO, NHTSA, FHWA, FMCSA, FTA.

DRAFT

- **Transportation Agencies[2]:** To be engaged in exploring certification processes, identifying needs and oversight. . Ultimately, these stakeholders will need to understand criteria and how to specify, within their procurements, the appropriately certified devices and equipment and will need to train their procurement and maintenance personnel. Stakeholders to be engaged through AASHTO, ITE, APTA, IBTTA and others as needed.
- **Vehicle Manufactures and Fleet Owners/Operators[3]:** To be engaged in exploring certification processes, identifying needs and oversight. Ultimately, these stakeholders will need to understand criteria and how to specify, within their procurements, the appropriately certified devices and equipment and will need to train their procurement and maintenance personnel. Stakeholders to be engaged through VIIC, CAMP, ATRI, APTA, CTAA and others as needed.
- **Device/Equipment Manufacturers**: To be engaged early in the process to help define the criteria and process against which their products will be tested and approved. Manufacturers include those producing embedded devices, aftermarket devices, roadside equipment. Stakeholders to be engaged through SAE, ITS America, SEMA, CEA, CVSA, ATRI, APTA and others as needed.

Stakeholder Outreach and Education:

The following stakeholders will likely be interested in participating in the process of becoming a certifying facility or entity. As such, they will need awareness of the effort, updates, and, eventually, a clear understanding of the criteria in order to determine whether they have a role in the ongoing certification process.

- **Standards Development Organizations:** Will be interested in understanding and contributing to the process development and in potentially becoming certification bodies. .
- **Certification Laboratories (Underwriters laboratories):** Will be interested in determining whether their facilities can meet the criteria and provide certification for devices and equipment.

Outcomes for Safety Pilot:

- A fully developed certification process to be used for the devices and equipment that will be part of Safety Pilot.
- An evaluation to identify what works and what needs further development.

Outcomes for NHTSA Regulatory Decision:

- A certification process needs to be defined as feasible in support of a regulatory decision.

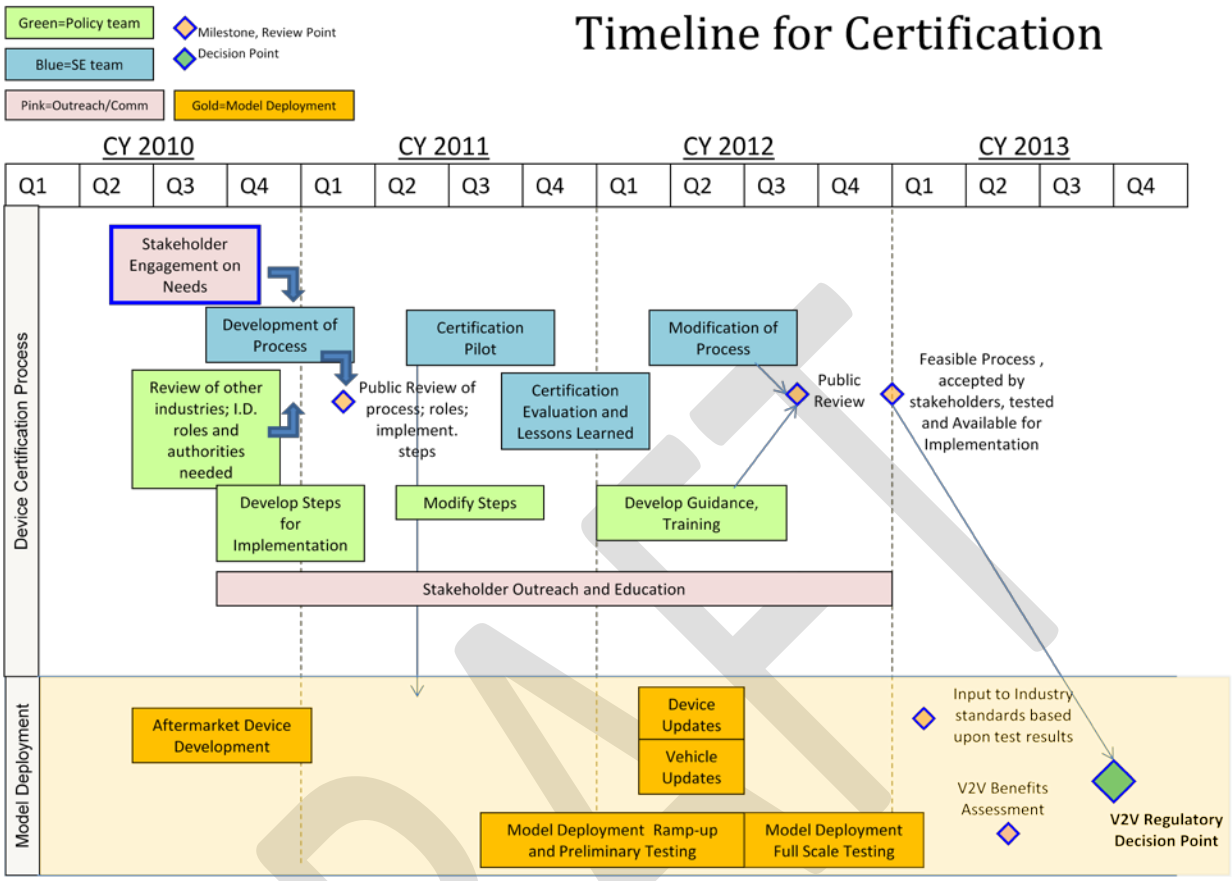
Outcomes for Deployment:

- An operational certification process with an oversight entity(ies) with the proper authorities.
- A set of laboratories/facilities available to certify devices and equipment.
- Guidance and/or training for agency personnel.

[2] Throughout this document, Transportation Agencies refers to operators of roadway, toll, transit, and rail facilities that may use IntelliDrive. This potentially includes light rail. At this time the potential value of IntelliDrive for heavy rail is still being determined.

[3] Throughout this document Vehicle Manufacturers and Fleet Owner/Operators refers to manufactures of light vehicles, trucks and busses and fleet owner/operators primarily for truck and transit systems, potentially including bus and light rail. At this time the potential value of IntelliDrive for heavy rail is still being determined.

Roadmap



B. CERTIFICATE AUTHORITY, CERTIFICATES, PRIVACY, AND SECURITY

A certificate authority is an entity that issues digital certificates that confirm or validate that the person, vehicle, organization, or other entity looking to access the system is a legitimate user. For IntelliDrive^{SM} Safety, certificates will need to be incorporated onto vehicles and into nomadic devices, and may also be needed as part of roadside equipment for spot safety. Common, existing certificate authorities (such as VeriSign) contain a public key (credential for trust) and the identity of the owner. Under IntelliDrive^{SM}, the goal is to design a ***highly secure credentialing process that offers anonymity for the user***.

Thus, security and privacy comprise two of the critical driving forces behind the design of a certificate authority and how certificates are issued for V2V and V2I. There exist a number of security scenarios, each having trade-offs with privacy, cost, scalability, and timing of deployment. The scenario that is ultimately chosen will result in a range of issues that will need to be addressed. Additionally, once a security scenario is chosen and a CA structure is designed, further analysis will be needed on such issues as enforcement and procedures to address bad actors.

Policy Questions

- **Designing a feasible CA:**
  - What types of entities should be allowed to act as a certificate authority (CA)? What is the role of the Federal government? Can industry or other institutions be allowed to act as a CA? What new authorities are needed? What are the requirements for establishing and operating a CA?
  - Would there be a single certificate authority (CA) or multiple? Multiple CAs may provide greater security and privacy—Is enhanced security worth the extra cost resulting from technical complexity?
  - Will the CA operator be the same for safety and for other applications? If not, how will they be coordinated?
  - How many times a year must a CA communicate with an OBE or RSE for updates?
  - If the public sector is involved in CA oversight, will the public sector have access to both public and private keys?
  - What are estimated costs for developing and operating the CA over time? What are potential business models for supporting these costs? Can these be a wholly private sector function?
- **Operating a CA:**
  - What types of legal instruments can be used to discourage potential misbehavior?
  - Who will monitor the system for misbehavior? How will misbehavior be detected (reported) and what are the actions to stop the misbehavior?
  - How can someone be removed from the system and how can they be reinstated?
- **Security:**
  - What are the potential security scenarios for IntelliDrive℠? What are trade-offs in terms of cost, privacy, and security? What are potential vulnerabilities in the system?
  - What security scenarios are desirable from the perspective of the vehicle manufacturers and fleet owner/operators? Nomadic device manufacturers? Transportation agencies? For what reasons?
  - Is the risk of a minimal security level acceptable for the first year of deployment? What is the probability of bad actors and what are the potential consequences?
- **Privacy:**
  - What level of privacy is acceptable for stakeholders? Will the CA design assure anonymity? If not, what personal information is vulnerable to identification? What are the consequences?
  - Will there be different privacy standards for vehicle data versus driver data?
  - Will aftermarket device manufacturers have access to proprietary data?
  - Will identifiers be eliminated within data to protect driver privacy?
  - What level of privacy is acceptable for opt-in applications versus all applications?
  - What data is stored and for how long? Who has access to it?
  - Are there any existing policies or laws that would challenge the V2V privacy model?

Tasks

- Work with security experts, conduct analyses on various security scenarios to understand trade-offs between different CA structures and cost, privacy, risk, scalability, etc.
- Engage stakeholders on the various security scenarios and understand desired options.
- Develop a recommended CA design that is either a single entity or multiple entities.

- Evaluate existing certificate authority organizations to understand how existing CAs operate. Engage experts to use inputs to design a CA structure, roles, responsibilities, authorities, operations, etc. that are relevant to IntelliDrive[SM].
- Based on security scenario analyses, identify what privacy information is vulnerable.
- Engage with privacy experts and review current laws and practices.
- Once a CA structure is defined, meet with privacy advocates to review whether privacy is adequately addressed to meet public and policymakers needs or if more needs to be done.
- Engage a broader group of stakeholders for validation/comment.
- Test CA as part of safety pilot. Evaluate and modify based on lessons learned.
- Develop a deployment timeline scenario and steps needed for CA implementation.

Stakeholder Collaboration:

The following stakeholders need to be considered as partners in developing or reviewing the process that is designed by experts:

- **Federal Government:** To lead and to be engaged in setting the criteria for security and privacy, and in understanding any ongoing Federal role. Stakeholders include ITS JPO, NHTSA.
- **Transportation Agencies :** To be engaged as part of the process in security and privacy and their role in the CA. Stakeholders to be engaged through AASHTO, ITE, APTA, IBTTA and others as needed.
- **Vehicle and Nomadic Device Manufacturers**: Will need to be engaged early in the process to help define security, the mechanism for certificate distribution and updates, and their role in CA as they may bear some risk for liability or will need to respond to a legal action if security is breached and unintended consequences result in injury or liability. Stakeholders to be engaged directly and through CAMP, VIIC, SAE, ITS America, SEMA, CEA.
- **Privacy Experts and Advocates**: Will need to be engaged early in the process to ensure that privacy is adequate to allow for deployment.

Stakeholder Outreach and Education:

The following stakeholders will need to understand the privacy issues or non-issues involved with deploying V2V and V2I for spot safety. In addition to privacy and access to personal data, the key points and messages need to be formulated to address “Big Brother” and enforcement issues:

- Leaders
- Citizens Groups

Outreach on these issues will be combined with broader outreach efforts on the concept and benefits. However message points need to be developed around these topics.

Outcomes for Safety Pilot:

- A CA will be designed and available for testing.
- Privacy experts and advocates will have been engaged to ensure that privacy will not be an obstacle to deployment.

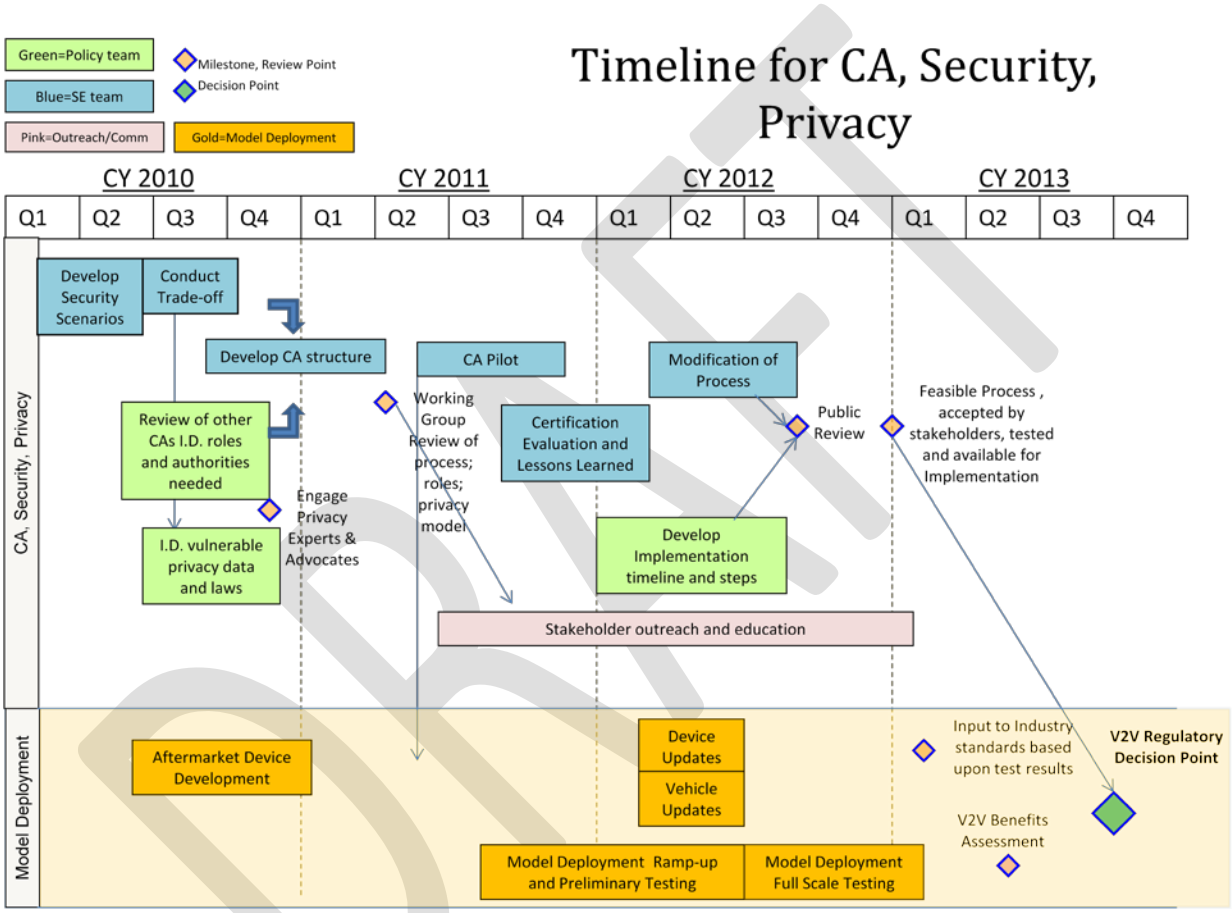
Outcomes for NHTSA Regulatory Decision:

- A feasible CA structure with security and privacy designed and validated with stakeholders.
- An identification of additional authorities needed for a CA entity.

Outcomes for Deployment:

- An operational CA structure.

Roadmap



C. RISK ALLOCATION AND LIABILITY / DATA OWNERSHIP

With the move to cooperative systems, the issue of liability and where risk resides with the delivery of safety advisories and warnings becomes fundamentally more complicated. The issue is further complicated by the introduction of nomadic devices and their potential future ability to tap into vehicle data. Retrofit devices may also introduce complexity.

The initial deployment of the basic safety message as part of the model deployment faces a more limited set of liability challenges. With the delivery of the basic safety message, how are vehicle or device manufacturers liable? Once applications and more complicated messages, in particular, messages developed from many sources of data, more complexity is added to the liability question (when data is

developed in a cooperative manner, how is risk allocated among the many players that own the data [and how does one determine data ownership?])

Finally, if NHTSA decides to issue a mandate for use of DSRC for safety, legal research will need to determine whether the basic safety messages and messages from applications can be covered under existing Federal liability statutes (immunity).

Policy Questions

- How is liability determined when collisions occur in a V2V environment using cooperatively produced data? How is risk allocated among data owners? Who are data owners and how/why are they responsible?
- How will liability be determined in driver error versus equipment error situations? What about driver distraction and the HMI? What about negligence or failure to heed warnings?
- If mandated, do existing liability laws cover these situations? If so, what is the role of the Federal government in exercising this authority for daily operations?
- Who owns what data and by what criteria? Who can use data and for what purposes? How would proper use be managed and controlled?
- When data passes through an algorithm that enhances the data, does ownership change?
- What data from the vehicle is made available to nomadic devices? What data should be made available and how does this shift risk allocation and liability?

Tasks

- Identify V2V data sets, origin points, algorithms used in basic safety message and applications.
- Identify where cooperative systems change the nature of data ownership.
- Engage legal experts to identify existing data ownership laws and practices. In particular, identify :
    - Cases involving transit data ownership going through the court systems now.
    - Liability conventions for conventional traffic control devices.
    - Existing government immunities similar to FAA systems or emergency systems.
- Engage risk allocation experts (i.e., insurance industry, legal firms) to develop a risk allocation model (how risk and liability can be legally and appropriately allocated among manufacturers, public agencies, and users of IntelliDrive^{SM} devices and equipment) for V2V and V2I for spot safety using both embedded devices and nomadic devices. Analyze impact to market opportunities.
- Engage with the insurance industry as a whole to determine impact to their business case and concerns they might have with the risk allocation model.

Stakeholder Collaboration:

The following stakeholders need to be considered as partners in developing or reviewing the process that is designed by experts:

- **Federal Government:** To scope out the issues that need further analysis and to engage experts. Stakeholders include ITS JPO, NHTSA, FHWA, FMCSA, FTA.
- **Legal (Technology) Firms and Trial Lawyers**: To identify existing laws and practices and apply to V2V and V2I environment. To identify whether existing government immunities and conventions for traffic control devices apply. To develop a risk allocation/liability model with identification of data ownership.
- **Vehicle Manufacturers and Device and Equipment Manufacturers**: To provide information on existing laws and practices from their legal teams as well as desired outcomes of the risk

allocation/liability model. To engage throughout the process to comment on model as it develops, and provide information on market impact. Stakeholders to be engaged directly and through CAMP, VIIC, SAE, ITS America, SEMA, CEA.

- **Transportation Agencies :** To provide input on efficacy of existing laws and practices with conventional traffic control devices. To be engaged on issues of data ownership. To be engaged throughout process to review options for IntelliDrive^{SM} safety risk/liability allocation and data ownership analysis. Stakeholders to be engaged through AASHTO, ITE, APTA, IBTTA and others as needed.
- **Universities/Evaluation Community:** Provide insights on relevant past and existing experiences and lessons learned. Stakeholders to be engaged through university outreach networks, IntelliDrive knowledge management tool and potential targeted discussions, meetings or projects.

Stakeholder Outreach and Education:

The following stakeholders will need to be educated on IntelliDrive^{SM} for safety and then engaged on how the above model might impact the industry:

- **Insurance Associations and Firms**: To have outreach provided to develop an understanding of IntelliDrive^{SM} for Safety. To be engaged in reviewing model and identifying vulnerabilities with model. To determine how risk allocation/liability model impacts existing models for insurance and impact to market.

Outcomes for Safety Pilot:

- An initial risk/liability model design.
- A review of government immunities and application to V2V environment (update of current legal analysis, but in a format for public consumption).

Outcomes for NHTSA Regulatory Decision:

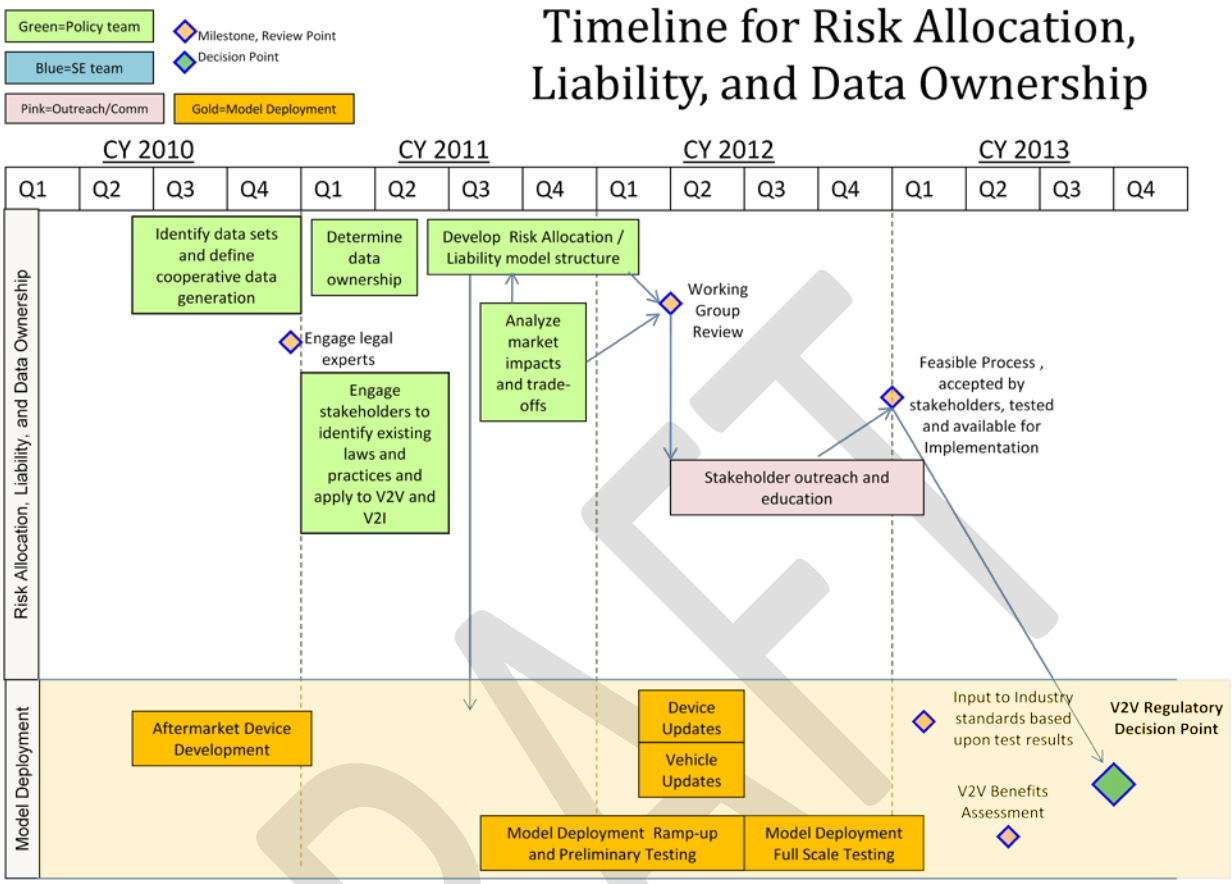
- Validated risk/liability model and economic impact analysis.
- Validated data ownership analysis.
- Potential incorporation of new immunities (if appropriate) as part of regulation.

Outcomes for Deployment:

- New legislation (if needed) for immunity (if appropriate).

DRAFT

Roadmap



D. COST-BENEFIT ASSESSMENT IN SUPPORT OF NHTSA REGULATORY DECISION

Cost-Benefit analysis is a critical tool in developing the basis for a regulatory decision. To result in a fact-based and evidence-based decision, a variety of analyses will be conducted to determine whether the benefits and costs of mandating DSRC and safety applications will result in significant benefits to the Nation.

Policy Questions

- What vehicle classes (passenger, commercial, transit vehicles, etc.) are to be included in a potential mandate?
- What data is necessary and when for supporting the regulatory decision process?
- How effective is the technology at reducing crashes? What technology if any needs to be mandated to obtain benefits?

- What are likely deployment scenarios and timeframes for use in estimated costs and benefits of a potential mandate? What are potential development and operating costs of any governance/oversight/operational entities needed?
- What type of benefits is this mandate expected to produce and what should be included in the cost/benefit analysis? Quantify the costs and benefits of a potential mandate.
- What is the cost-effectiveness of the different integrated V2V safety applications alone and by comparison to alternative countermeasures such as stand-alone applications, roadway redesign, signs, etc.?
- How will the cost of mandating DSRC impact the Nation? Agencies? Manufacturers? Citizens?

Tasks

- Work with the developers of the V2V safety applications to develop a model for analyzing cost and effectiveness. Develop assumptions and constraints.
- Validate model with public working group.
- Analyze each application with existing data on costs and benefits gathered from stakeholders, previous tests, and NHTSA and FHWA safety databases (or other Federal databases).
- Compare each application to alternative countermeasures.
- Work with NHTSA office for rulemaking to develop a process and timeline for gathering the right data at the right time for a regulatory decision.
- Gather data from Safety Pilot to revise analyses.
- Determine potential costs or benefits from the way the certification and the CA is structured, the application of standards, the manner in which risk is allocated, the ownership of data, the punitive aspects of enforcement, etc.
- Work with stakeholders to identify the various players that may be impacted by the mandate.
- Conduct economic impact analysis to agencies, manufacturers, citizens and others.
- Formulate data-based options for NHTSA.

Stakeholder Collaboration:

The following stakeholders need to be considered as partners in developing or reviewing and validating the process that is designed by experts:

- **Federal Government:** To build the model. To collaborate with industry and State and local agencies on developing model, assumptions, constraints, costs, and benefits.
- **Industry:** To provide data inputs to the process.
- **Transportation Agencies:** To provide data inputs to the process based on what vehicle classes are included in the mandate.

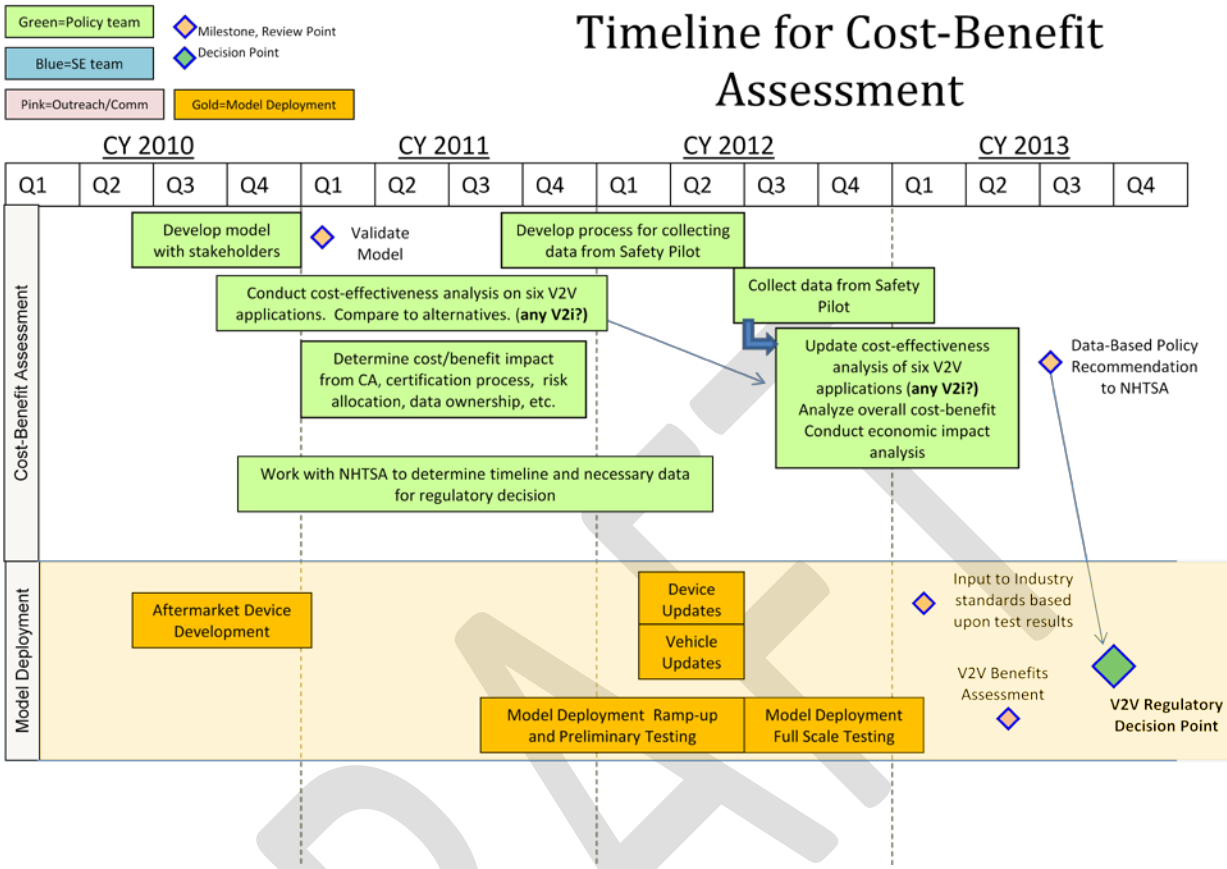
Outcomes for Safety Pilot:

- Cost-benefit and cost-effectiveness models established (assumptions, constraints, and initial costs) and validated with stakeholders.
- Cost-effectiveness analyses conducted on individual safety applications.
- Determination of what data is needed from Safety Pilot and process for collecting, organizing, scrubbing, and using data.

Outcomes for NHTSA Regulatory Decision:

- Full cost-benefit analysis in format useful for NHTSA regulatory decision.
- Agency, industry, citizen economic impact analysis.

Roadmap



E. RULES OF OPERATION AND APPLICATION OF STANDARDS

With a nationwide system, consistency (especially across jurisdictions) and interoperability (especially across different vehicle makes and models) need to be both assured and enforced. These are achieved through common rules of operation and use of standards.

Policy Questions

- **Rules of Operation:**
  - What rules are needed to ensure safe, secure, appropriate operations of the system as the system crosses jurisdictional lines? Who will design and enforce these rules? Who will monitor for misbehavior?
  - Is it possible for any of the rules to have flexibility to tailor to the local needs? If so, which ones?
  - Who will be allowed or not allowed to use the channel reserved for safety messages? What will be the rules to use the safety channel of the spectrum? How will safety messages be prioritized?
  - How will a safety vs. a non-safety message be determined?

- **Standards:**
    - Is an official body needed to select and sanction standards for use on the system? How will decisions be made about the need for upgrades or new standards? How will decisions be made about adoption among competing standards?
    - Which entities will issue standards?
    - Who will enforce use of standards? How? Is new authority needed?
    - Will there be a single set of technical standards that apply to vehicles and infrastructure? Will they be federally mandated standards? For instance, if a local government is using its own funding to install RSE, will federal standards still apply?
    - What are the appropriate roles of the Federal government, transportation agencies, and industry?
    - What types of data standards are necessary to ensure interoperability?
    - Will similar standards apply to OEMs versus aftermarket device manufacturers?
    - Will standards be harmonized for global marketplace adoption?
- **Enforcement:**
    - What aspects of the system require enforcement?
    - How is "fraudulent" or "mis-use" defined?
    - What are system tools for monitoring and enforcement? Do they violate privacy principles? Who will do the enforcing?
    - What type and level of authority does NHTSA have for enforcement? What is the role of the FCC in enforcement?
    - Will the system build in mechanisms for apprehension and criminal prosecution of fraudulent messages? How?
    - What are the necessary laws that need to be passed?
    - What are operational requirements for any enforcement or standards oversight/management entities needed? What are estimated costs for establishing and operating these entities? What are potential institutional models for these functions? Can this be a wholly private function?

Tasks

- Review rules of operations for other multi-jurisdictional systems to determine how the rules of operations where developed and the lessons learned from the experience.
- Through governance structure development, identify who will have the authority to develop and enforce rules of operations and use of standards.
- Engage stakeholders to develop rules of operations.
- Identify whether the device certification process deals with the issue of use of standards or if more is needed beyond the certification process.
- Determine appropriate roles and responsibilities in standards setting.
- Pursue international harmonization of standards.
- Engage legal experts to define terminology and identify whether and what type of actions would fall into the "illegal" or "misuse" category.
- Engage system developers and security experts to determine whether mechanisms can be build into the system to identify misuse and to apprehend and prosecute abusers. Determine whether these mechanisms violate privacy principles.
- Develop toolbox of enforcement techniques. Analyze State and local legislation to determine if new laws will be in conflict or if existing laws prohibit enforcement.
- Determine operational requirements, costs and institutional models.

Stakeholder Collaboration:

The following stakeholders need to be considered as partners in developing or reviewing the process that is designed by experts:

- **Federal Government:** To facilitate stakeholder engagement on rules of operations, requirements for enforcement, and toolbox of enforcement techniques.
- **Systems Developers:** To determine whether apprehension and enforcement mechanisms can be built into the system without violation of privacy.
- **Privacy Advocates:** To ensure that privacy is protected. To help set requirements for balancing the need for system enforcement against privacy.
- **Transportation Agencies, Manufacturers, Industry:** To be engaged in setting requirements for rules of operations.
- **Standards Development Organizations:** To help define roles and responsibilities in standards setting.
- **International Standards Organization:** To facilitate international harmonization.

Outcomes for Safety Pilot and Model Deployment:

- A prototype set of rules of operations to test within model deployment.
- Enforcement (monitoring, apprehension, prosecution) systems built into prototype system to test under model deployment conditions.
- Completion of standards and process for upgrading/maintenance in place.

Outcomes for Deployment:

- Internationally harmonized standards.
- Toolbox of enforcement tools including new model legislation, if needed.

Roadmap

F. SPECTRUM ANALYSIS AND FCC ROLE

The IntelliDrive^{SM} safety program will most likely use the 5.9GHz space of the communications spectrum and as a result, could be subject to the regulations provided by the FCC. It will be crucial to understand how the 5.9GHz spectrum will be allocated and managed as well as the process by which different entities will be able to license the spectrum (have access).

Policy Questions

- Is a spectrum manager needed? If so, who will be the spectrum manager? What are the roles and responsibilities for spectrum management?
- How will the definition of a governance entity(ies) define or include spectrum management?
- How does the role of spectrum manager overlap with or address rules of operation, enforcement, standards setting, etc?
- How will the FCC assure valid use and non-interference?

Tasks

- Understand the process by which the FCC currently regulates spectrum use and identify issues

unique to IntelliDrive[SM.]

- Define the requirements for spectrum manager and determine which entities meet the requirements. Define a process for determining the spectrum manager if more than one entity meets the criteria.
- Discuss use of the spectrum with FCC and present plans for V2V and V2I for spot safety. Present plans for rules of operation and enforcement to understand how the FCC might play a role. Present plans for governance. Elicit feedback from FCC.
- Discuss the processes in place for FCC to assure valid use and non-interference.
- Determine the current process for licensing agencies and other entities to use the spectrum (FHWA Turner Fairbanks has been facilitating the process). Determine whether the process will work for the long-term or if a different process needs to be established.

Stakeholder Collaboration:

The following stakeholders need to be considered as partners in developing or reviewing the process that is designed by experts:

- **FHWA**: Engage FHWA on the existing licensing process and determine whether the process will work for the longer-term.
- **FCC**: Engage the FCC on the range of issues described above and work to understand the FCC role and responsibilities.
- **Vehicle manufacturers and fleet owners/operators, transportation agencies, device and equipment manufacturers**: Engage wide range of stakeholders on the requirements for a spectrum manager.

Outcomes for Safety Pilot:

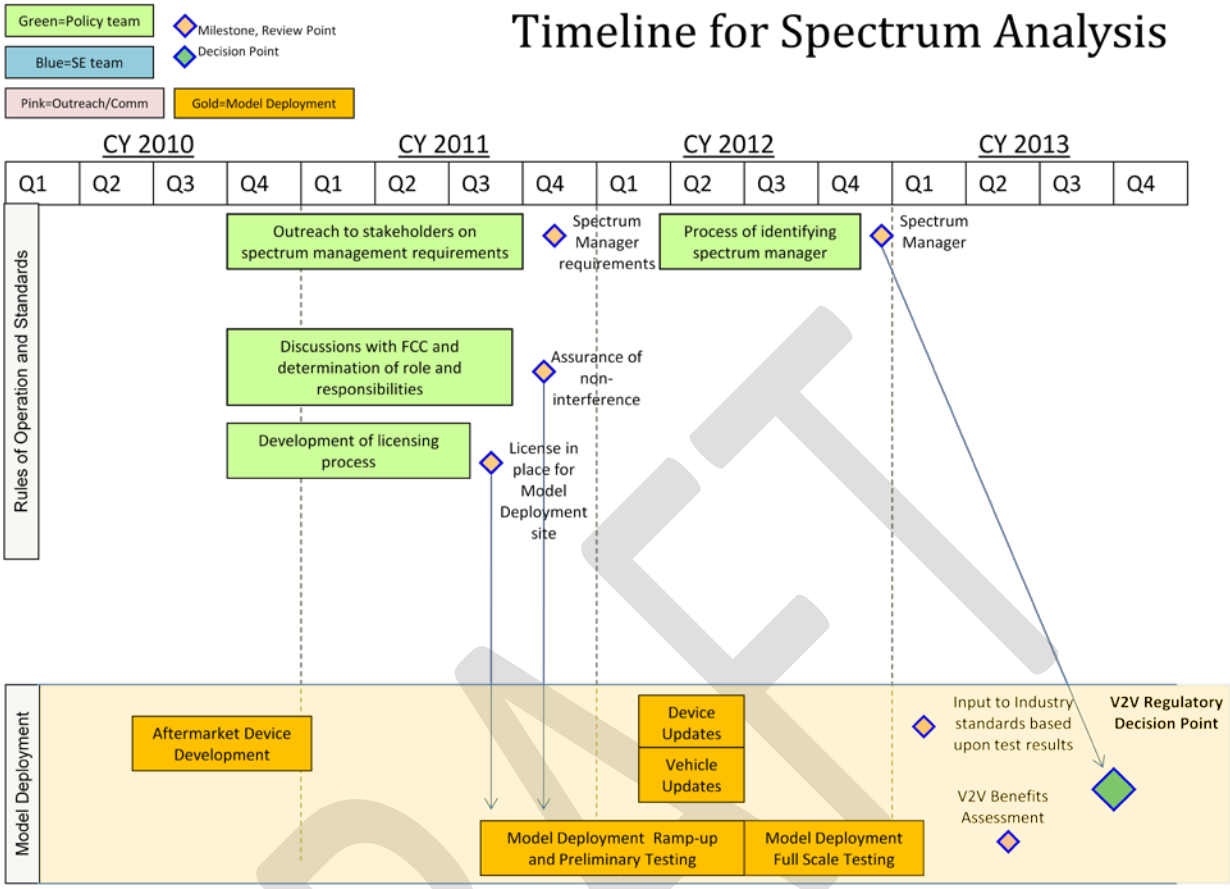
- Clear understanding of the licensing requirements.
- Clear understanding of FCC role.

Outcomes for NHTSA Regulatory Decision and for Deployment:

- Determination of spectrum manager and analysis of impact of the choice upon industry.
- Determination of FCC role and responsibilities.

Roadmap

DRAFT



G. INFRASTRUCTURE

IntelliDrive[SM] Safety includes both V2V and V2I interactions. For V2V, there needs to be a determination regarding whether and what type of infrastructure will be required for security and certificate authority processes. For V2I, there are a number of safety applications that will require infrastructure. From a policy perspective, there are numerous issues regarding funding, deployment, and maintenance of infrastructure that are similar to other ITS infrastructure issues but may need to be tailored to meet the needs of a multi-jurisdictional IntelliDrive[SM] system.

Policy Questions

- Can we take advantage of existing systems for infrastructure/roadside equipment? If so, how? If not, what infrastructure needs to be developed for security and for V2I spot safety? What is minimum level to achieve maximum benefit?
- Who will be responsible for setting up and maintaining the required roadside equipment? Who will finance this equipment? How?
- Who will be responsible for setting up and maintaining the required connections from the roadside equipment to the certificate authority? Who will finance this necessary function?

Tasks

- Determine whether roadside equipment is needed for security and, if so, how much and where the likely placement will be.
- Engage AASHTO members to identify issues with roadside equipment and O&M.
- Address upgrades to technologies as part of governance structure.

Stakeholder Collaboration:
The following stakeholders need to be considered as partners in developing or reviewing the process that is designed by experts:

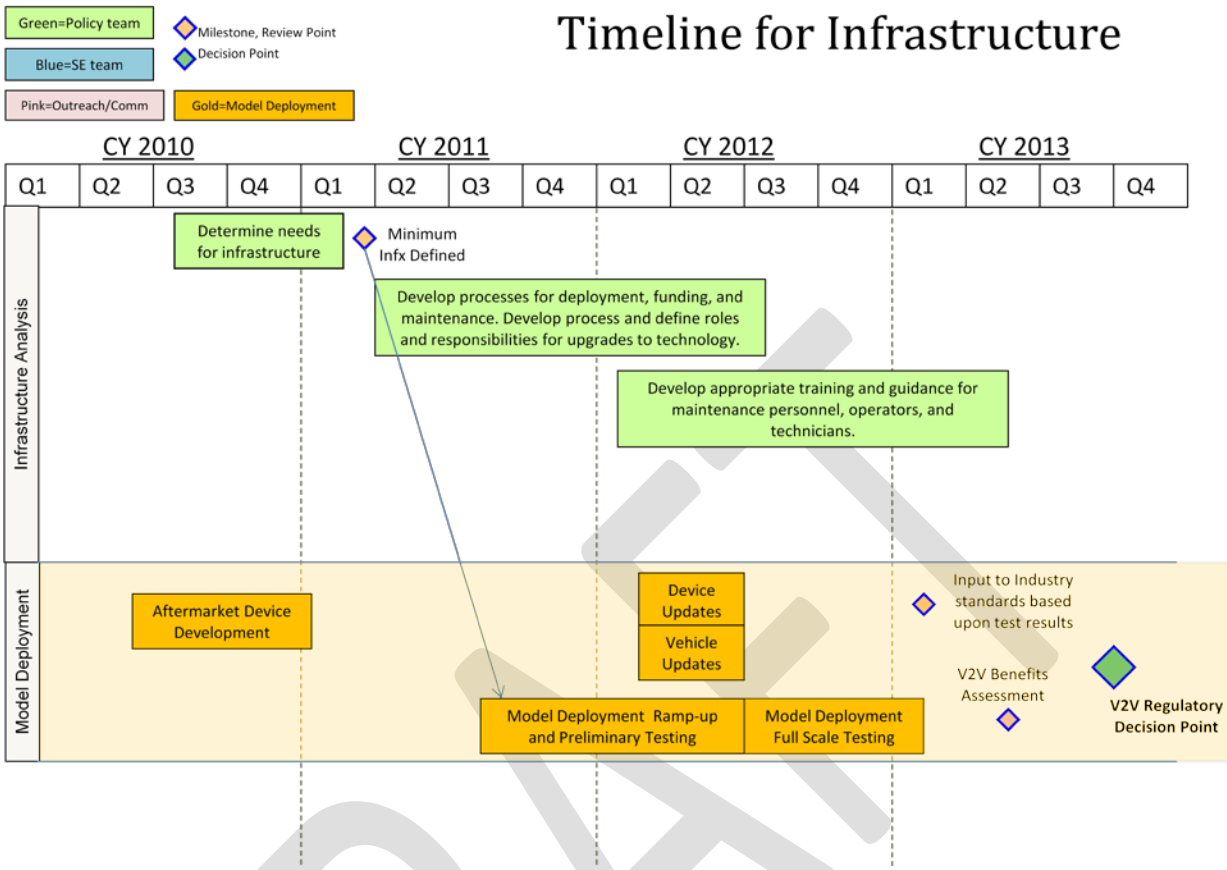
- **Federal Government:** To engage key stakeholders in determining the minimum amount of infrastructure requirements.
- **Transportation Agencies:** To define the processes by which IntelliDrive^{SM} infrastructure gets deployed, maintained, and funded.
- **Vehicle Manufacturers and Security Experts:** To define the level of infrastructure needed for security and certificate authority purposes.

Outcomes for Safety Pilot:
- A design for infrastructure for security and certificate authority, if needed.

Outcomes for Deployment:
- A set of processes for funding, deployment and maintenance of IntelliDrive^{SM} infrastructure.

Roadmap

DRAFT



H. GOVERNANCE STRUCTURE AND AUTHORITY

A governance structure defines the type and level of authorities needed for V2V and V2I deployment, system operations, and enforcement, and defines the roles and responsibilities of the players engaged in the system. All of the previous elements defined in this paper (Sections A-G) comprise key elements of the system (or daily) governance needed for IntelliDrive^{SM}; a governance structure, however, also must be defined at a higher level to address more global roles and responsibilities. The goal under this focus area is to combine the options generated from research under A-G into a feasible governance structure(s) for IntelliDrive^{SM} Safety.

Policy Questions

- Is a governance structure necessary? What aspects of IntelliDrive require governance (as distinct from those aspects that the private sector should be allowed to work out on its own)? Is it one governing body or multiple? Federal, private, or both?
- Is there a structure for regional governance?
- What authorities need to be granted? For what purposes?
- What type of entity(ies) will be most effective for oversight, operations, and enforcement?
- How will the entity(ies) balance competing needs? Resolve conflicts? Shield the system and the players from political shifts? Sustain itself?
- What roles are OEMs not allowed to participate in due to anti-trust issues?

- Are existing governmental structures for safety regulation and enforcement applicable to (and sufficient for) IntelliDrive?
- Do existing safety agencies have the necessary authority to govern IntelliDrive? If not, will new enabling legislation be required?
- What is the appropriate division of authority and responsibility among federal, state, and local entities?
- How are key stakeholders likely to be affected by various IntelliDrive governance models?
- How will the governing entity track and address system misuse or misbehavior?
- Do strategies for retrofit or aftermarket require any different governance?
- What are operational requirements for any governance entities? What are estimated costs for establishing and operating these entities? What are potential institutional models for these functions? Can this be a wholly private function?

Tasks

- Review governance structures of other entities. Models span range from full legal oversight authorities to authority granted by consensus of users. Examples to include: Energy Star (govt/industry partnership), WiFi Alliance and BlueTooth SIG (industry led), WWW (volunteer), Next Gen (govt)
- Identify governance experts who know how to structure entities. Work with them to:
    - Identify governance structures of other organizations and relevant features;
    - Identify technically feasible approaches for centralized and/or distributed certificate authority operations (B);
    - Identify technically feasible approaches for the certificate authorities and vehicles to communicate (B);
    - Investigate the effectiveness and cost/benefits of having centralized versus distributed CA system (A);
    - Identify how to incorporate rules of operations and standards into a governance structure (E)
    - Identify enforcement options and tools for incentives or punitive measures (E).
    - Identify economic and market impacts of various structures (D)
    - Identify authorities and how governance structure affects liability and risk (C).
- Develop option(s) for V2V governance structure with key stakeholders – incorporate elements from research on Certificate Authority, Device Certification, Privacy, Liability, Data Ownership, and Cost-Benefit Analysis.
- Develop and hold a governance experts workshop in Fall/Winter 2010. Revise plans based on input and continue to develop further detail. Provide prototype governance structure for testing. Hold second workshop in 2012 with the intention that the definition of the governance structure mostly complete and available for incorporation into the NHTSA regulatory decision.
- Determine operational requirements, costs and institutional models.

Stakeholder Collaboration:

The following stakeholders need to be considered as partners in developing or reviewing the process that is designed by experts:

- **Federal Government:** To coordinate the research, engage experts, and facilitate dialogue among the governmental and industry players that will be impacted by the governance structure.

- **Transportation Agencies and Industry:** To participate in the process and provide input on needs.
- **Experts**: To identify how governance works in other industries and provide expert advice on how to structure a governance entity(ies) for IntelliDrive^{SM}.

Stakeholder Outreach and Education:

The following stakeholders will need to understand the governance structure and how it will work, its impact on citizens, and the processes for access to the IntelliDrive^{SM} system:

- Leaders
- Citizens Groups

Outcomes for Safety Pilot:

- A prototype governance structure to be tested during testing

Outcomes for NHTSA Regulatory Decision:

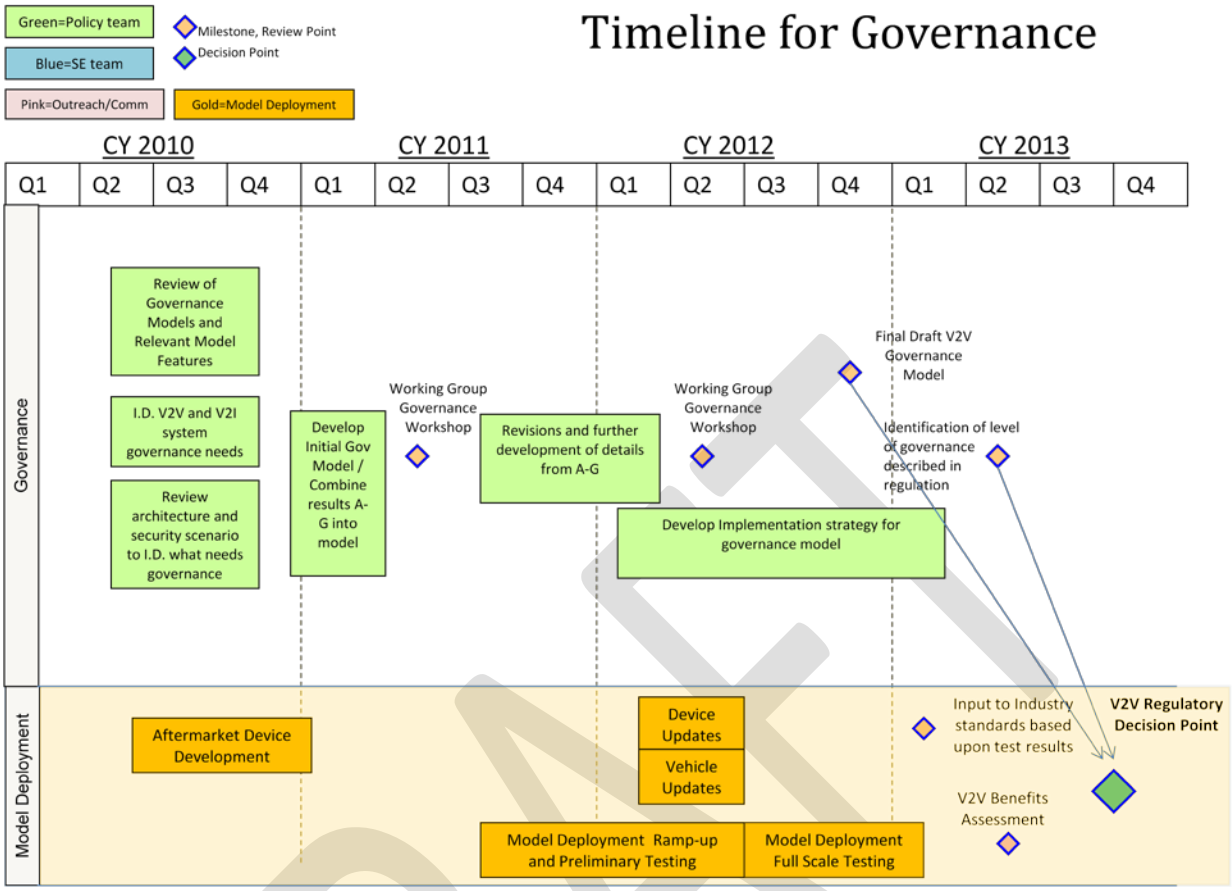
- A validated, feasible governance structure in support of V2V and V2I for spot safety

Outcomes for Deployment:

- A working governance entity

Roadmap

DRAFT


Timeline for Governance
Green=Policy team
Blue=SE team
Pink=Outreach/Comm
Gold=Model Deployment
Milestone, Review Point
Decision Point
CY 2010
CY 2011
CY 2012
CY 2013
Q1 Q2 Q3 Q4 Q1 Q2 Q3 Q4 Q1 Q2 Q3 Q4 Q1 Q2 Q3 Q4
Governance
Review of Governance Models and Relevant Model Features
I.D. V2V and V2I system governance needs
Review architecture and security scenario to I.D. what needs governance
Develop Initial Gov Model / Combine results A-G into model
Working Group Governance Workshop
Revisions and further development of details from A-G
Working Group Governance Workshop
Develop Implementation strategy for governance model
Final Draft V2V Governance Model
Identification of level of governance described in regulation
Model Deployment
Aftermarket Device Development
Device Updates
Vehicle Updates
Model Deployment Ramp-up and Preliminary Testing
Model Deployment Full Scale Testing
Input to Industry standards based upon test results
V2V Benefits Assessment
V2V Regulatory Decision Point

DRAFT