OVERVIEW OF THE INTELLIDRIVE POLICY PROGRAM

IntelliDriveSM is a multimodal initiative that aims to enable safe, interoperable, networked wireless communication among vehicles, roadside infrastructure, and passengers’ personal communications devices. The IntelliDrive Program is a multi-faceted research program that includes research around three key areas:

- **IntelliDrive Safety:**
  - Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I) for Safety
  - Safety Pilot

- **IntelliDrive Mobility:**
  - Data Capture and Management Systems
  - Dynamic Mobility Applications

- **IntelliDrive Environment:**
  - Applications for the Environment: Real-Time Information Synthesis (AERIS)
  - Road Weather Applications

Each of these programs has a technical research and policy research component. This program is meant to be multi-modal and a specific focus is given to identifying and addressing technical requirements and policy issues related to transit and trucks within each of these programs. This document is the first of six policy roadmaps that will outline the policy and institutional issues across all of the IntelliDrive research programs. Policy issues will be identified using the following approaches:

- **Evaluating Technical Policy Issues:** Refers to policy issues that are specific to a technical area and that support the continuation of technical research. As the technical team conducts its research, specific policy questions and issues arise. Generally, these issues emphasize the need for either a policy decision, validation of a policy assumption, or further research in order to continue moving the technical program forward. It is important to identify these technical policy issues as a way to support assumptions around technical configurations and to develop options for stakeholders to review. Using this approach, specific policy roadmaps will be developed for each of the research programs and will also align with each of the technical research roadmaps for those same programs.

- **Evaluating Global Policy and Institutional Issues:** Refers to policy issues that are global in nature and cut across all IntelliDrive Program areas. These policy and institutional issues focus on the governance, investments/financing, and institutional issues in support of IntelliDrive deployment. It is important to evaluate these issues from a global context because they overlap multiple policy and technical areas. These issues are described in greater detail in the IntelliDrive Policy Roadmap (Version 8, December 2010, which is posted at: [http://www.intellidriveusa.org/research/policy.php](http://www.intellidriveusa.org/research/policy.php)).

---

1 This document was first released on May 19, 2010 for comment. This version incorporates comments from numerous stakeholders and industry representatives. This second draft forms the basis for a presentation at an IntelliDrive Safety Program workshop on July 20-22, 2010. Comments from this workshop will be used to produce a final version of this roadmap which will guide V2V and V2I policy research.
OVERVIEW OF THE SAFETY POLICY ROADMAP

The purpose of this document is to describe a roadmap for conducting policy research under the IntelliDrive Safety Program (V2V and V2I). The document outlines critical policy areas and their relevant research questions, tasks, stakeholders, and outcomes. The policy research will be prioritized and driven by three key milestones within the V2V and V2I Programs:

- **Safety Pilot**: The Safety Pilot represents an upcoming opportunity to test and create a model deployment for V2V and some limited V2I technologies under real-world conditions. Certain policy questions and issues must be resolved in support of the Safety Pilot and these issues should be addressed in the near term and in coordination with Safety Pilot activities.
- **2013 NHTSA Regulatory Decision for Vehicle Communication Safety Systems**: NHTSA has committed to conducting the evaluation for making a regulatory decision on vehicle communications in 2013. The decision process will require a rigorous evaluation of the research results. The goal of the Safety Policy Roadmap is to support the development of the relevant policy research results and options in support of NHTSA’s evaluation.
- **Deployment**: Policy questions and issues must be resolved in support of actual deployment of V2V and V2I Safety.

POLICY AREAS

In deconstructing the V2V, Safety Pilot, and V2I technical research roadmaps, the following list of critical policy and institutional issues are defined in this Safety Program Policy Roadmap. Under each policy area, there will be a list of key policy questions, research tasks, stakeholders, and expected outcomes.

The general research area categories of policy issues include:

A. Device and Equipment Certification
B. Certificate Authority for Security
C. Risk Allocation and Data Ownership
D. Cost-Benefit Analyses in Support of Deployment
E. Rules of Operation and Application of Standards
F. Spectrum Analysis and FCC Role
G. Infrastructure for V2V and V2I Spot Safety
H. Governance Structure and Authority
Certification provides a process that ensures all devices and equipment connecting to the IntelliDrive system meet specific standards (criteria) relating to security, performance, and privacy. All equipment and devices used to send and receive communications for V2V and V2I Safety should be validated or certified by a certifying entity. The purpose of certification is to preserve safety and to protect interference of safety in IntelliDrive equipment and devices. This policy area addresses questions around identifying property certifying entities and ensuring an appropriate certification process.

1. Policy Questions

Certification Entity

- What types of entities should oversee the certification process and provide certification?
- Would a centralized (single source) or decentralized model be appropriate for the certification process?
- What types of entities will enforce the "certification"?
- Who will develop the certification requirements, tests, and standards?
- What is the role of the Federal government in ongoing certification, if any?
- Is any new authority needed to oversee IntelliDrive device and equipment certification?

Certification Process

- What IntelliDrive device and equipment needs to be certified?
- What are potential device and equipment certification processes? What are the certification criteria (standards for security, performance, and privacy) against which devices and equipment will be tested?
- Should there be different certification for V2V and V2I?
- Will there be a distinct process for aftermarket equipment? How will security requirement be met for aftermarket devices? What are potential certification processes for retrofit and aftermarket equipment (in order to ensure the security of proprietary vehicle systems)?
- Do existing certification laboratories for other industries provide any opportunities or lessons learned for IntelliDrive?
- What are the institutional models for operating a device and certification process? Can this be a wholly private sector function?
- Can self-certification and 3rd party certification recognition co-exist for C devices/systems?
- What is the re-certification timeframe?
- Do certification requirements need to be harmonized internationally? What is the process for this?
- How will the certification process ensure interoperability?
- Will there be a distinct process for roadside equipment (RSE)?
- How does the equipment replacement cycle impact IntelliDrive and/or aftermarket equipment?
- How can automated self monitoring be used to enable devices to self report invalid use?

2. Research Tasks

- Review certification processes from other industries to identify lessons learned, opportunities, authorities needed, and role of the Federal government. Possibly evaluate international examples.
• In collaboration with the IntelliDrive Systems Engineering Program, develop a certification process, certification criteria, and tests. Consult with certification experts and stakeholders (manufacturers of vehicles, devices, and equipment and SDOs).
• Review proposed certification process in collaboration with stakeholders.
• Conduct a certification pilot study in early 2011 as part of the Safety Pilot.
• Based on lessons learned from the certification pilot study, modify the certification process.
• Conduct stakeholder outreach, education, and collaboration during the development and testing of the certification process.
• Develop a plan for implementing a certification process, which will include identification of certifying entities.
• Identify international certification needs, to evaluate potential for international harmonization.

3. Stakeholder Collaboration:
The following stakeholders are considered full participants and are directly engaged in research tasks and development:

• **Federal Government**: Will be engaged to explore certification processes, identify needs and oversight. Stakeholders include ITS JPO, NHTSA, FHWA, FMCSA, FTA.
• **Transportation Agencies**: Will be engaged to explore 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. They will also need to train their procurement and maintenance personnel. Stakeholders include AASHTO, ITE, APTA, IBTTA and others as needed.
• **Vehicle Manufactures and Fleet Owners/Operators**: Will 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, SEMA, CEA, CVSA, ATRI, APTA and others as needed.

4. Stakeholder Outreach and Education:
The following stakeholders are indirectly engaged in research development and tasks and will act as informational resources. Ongoing education and outreach of research activities will be communicated with these stakeholders.

• **Standards Development Organizations**: Will be interested in understanding and contributing to the development of the certification process and in potentially becoming certification bodies.
• **Certification Laboratories**: Will be interested in determining whether their facilities can meet the criteria of becoming a certifying body and provide certification for devices and equipment.

---

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 Owners/Operators refers to manufacturers 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.
5. Outcomes for Safety Pilot:
   • A model certification process that will certify devices and equipment used during the Safety Pilot.

6. Outcomes for NHTSA Regulatory Decision:
   • A recommended certification process for devices and equipment. The process will have been tested during the Safety Pilot. Includes recommended input on certifying entities, roles and responsibilities.

7. Outcomes for Deployment:
   • An operational device certification and enforcement process. The process will include a recommended oversight entity and enforcement mechanism.
   • A set of laboratories/facilities available to certify devices and equipment.
   • Guidance and/or training for agency personnel.
   • Standard hardware specifications for built-in, retrofit, aftermarket, and field devices.

8. Roadmap

Device and Equipment Certification

<table>
<thead>
<tr>
<th>CY 2010</th>
<th>CY 2011</th>
<th>CY 2012</th>
<th>CY 2013</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q1</td>
<td>Q2</td>
<td>Q3</td>
<td>Q4</td>
</tr>
<tr>
<td>Stakeholder Engagement on Needs</td>
<td>Certificate Pilot</td>
<td>Certification Evaluation and Lessons Learned</td>
<td>Modification of Process</td>
</tr>
<tr>
<td>Process Development</td>
<td>Certification Pilot</td>
<td>Certification Evaluation and Lessons Learned</td>
<td>Modification of Process</td>
</tr>
<tr>
<td>Review of other industries, international examples, and I.D. Federal role</td>
<td>Device and Equipment Certification</td>
<td>Certification Process available for implementation</td>
<td>Certification Process available for implementation</td>
</tr>
<tr>
<td>Aftermarket Device Development</td>
<td>Device Updates</td>
<td>Vehicle Updates</td>
<td>Input to Industry standards based upon test results</td>
</tr>
<tr>
<td>Model Deployment</td>
<td>Model Deployment Ramp-up and Preliminary Testing</td>
<td>Model Deployment Full Scale Testing</td>
<td>V2V Regulatory Decision Point</td>
</tr>
</tbody>
</table>
B. CERTIFICATE AUTHORITY FOR 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 Safety, certificates will need to be incorporated onto vehicles and into aftermarket devices, and may also be needed as part of roadside equipment for V2I safety applications. Common, existing certificate authorities contain a public key (credential for trust) and the identity of the owner. The objective of this policy area 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 are 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 security and privacy 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 system misuse.

1. Policy Questions

CA Design:
- 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?
- What is the potential governance and/or ownership structure of a CA?
- How many times a year must a CA communicate with an OBE or RSE for updates?
- How will access to public and private keys operate, especially for the public sector?
- What are estimated costs for developing and operating the CA over time? What are potential business models for supporting these costs? Can this be a wholly private sector function?

CA Management:
- What are the basic operating procedures and protocols that will be used by the 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?
- What enforcement tools will be used?
- How can someone be removed from the system and how can they be reinstated?
- How will misbehavior caused by equipment error be handled?
- How do people obtain new certificates? How do you refresh a certificate?
- Is the CA going to be the entity that takes action?
Security

- What are the potential security scenarios for IntelliDrive? What are trade-offs in terms of cost, privacy, and security? What are potential security risks or threats to the system?
- What security scenarios are desirable from the perspective of the vehicle manufacturers and fleet owner/operators? Aftermarket device manufacturers? Transportation agencies? For what reasons?
- What level of security is acceptable for the first year of deployment? At what point do we address security differently than we would at day one?
- What is the probability of system misuse and what are the potential consequences?
- At what point do we need to have a final CA policy/system in place based on percentage of adopters?
- What types of penalties and/or enforcement tools are available for repeated misbehavior?
- What types of enforcement mechanisms are available to the CA? What is not available?
- How will vehicle systems remain secure when aftermarket equipment is used?

Privacy:

- What level of privacy is acceptable for stakeholders? Will the CA design assure an acceptable level of anonymity that also sufficiently addresses enforcement requirements? If not, what personal information is vulnerable to identification? What are the consequences?
- Will there be different privacy standards for different uses and/or data owners?
- 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 mandated [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?
- Who has liability for a certificate validity – counterfeiting?

2. Research Tasks

Certificate Authority

- Work with security experts, conduct analyses on various security scenarios to understand trade-offs between different CA design and cost, privacy, risk, scalability, etc.
- Engage stakeholders on various security scenarios to identify needs and desired options.
- Develop a recommended CA design that is either a single entity or multiple entities.
- Conduct evaluation of existing certificate authority organizations for comparative purposes.
- Engage experts to provide inputs for designing a CA design, roles, responsibilities, authorities, operations, and management.

Privacy & Security

- Based on security scenario analyses, identify the types of privacy information that is vulnerable.
- Discuss with privacy experts to review current laws and practices.
- Once a CA is designed, meet with privacy advocates and review whether privacy is adequately addressed to meet public and policymakers needs.
- Meet with 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.
• Evaluate existing privacy policies from a constitutional and commercial perspective.

3. Stakeholder Collaboration:
The following stakeholders are considered full participants and are directly engaged in research tasks and development:
• **Federal Government:** Will lead and be engaged in setting the criteria for security and privacy. Will provide input on any ongoing Federal (US DOT) role. Stakeholders include ITS JPO, FHWA, FTA, FMCSA, RITA, NHTSA.
• **Transportation Agencies:** Will be engaged as part of the process in security and privacy and their role in the CA. Stakeholders will be engaged through AASHTO, ITE, APTA, IBTTA and others as needed.
• **Vehicle and Aftermarket 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. They may bear some risk for liability or may need to respond to a legal action if security is breached and unintended consequences result in injury or liability. Potential 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 there are not major obstacles to deployment due to privacy issues.

4. Stakeholder Outreach and Education:
The following stakeholders are indirectly engaged in research development and tasks and will act as informational resources. Ongoing education and outreach of research activities will be communicated with these stakeholders.
• Privacy Advocates
• Citizens Advocacy Groups

5. Outcomes for Safety Pilot:
• A model certificate authority that will be able to provide authentication and credentialing during the Safety Pilot.

6. Outcomes for NHTSA Regulatory Decision:
• A feasible CA design with appropriate security and privacy levels.
• An identification of additional authorities needed for a CA entity.
• An assessment of privacy related issues that could act as an obstacle to deployment.

7. Outcomes for Deployment:
• An operational CA design.

8. Roadmap
Certificate Authority for Security

<table>
<thead>
<tr>
<th>CY 2010</th>
<th>CY 2011</th>
<th>CY 2012</th>
<th>CY 2013</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q1</td>
<td>Q2</td>
<td>Q3</td>
<td>Q4</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Q1</td>
<td>Q2</td>
<td>Q3</td>
<td>Q4</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Q1</td>
<td>Q2</td>
<td>Q3</td>
<td>Q4</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Stakeholder outreach and education**

- Develop Security Scenarios
- Conduct Trade-off Analysis
- Develop CA design for testing
- Test CA Model
- Modify CA Model

**CA Analysis (review existing examples)**

- Engage Privacy Experts
- Engage CA experts for input into CA design, roles, responsibilities

**Privacy analysis (determine privacy levels)**

- Develop CA implementation timeline and steps.
- Model Deployment Ramp-up and Preliminary Testing
- Model Deployment Full Scale Testing
- Provide input to industry standards based upon test results
- V2V Regulatory Decision Point
- V2V Benefits Assessment

**Model Deployment**

- Aftermarket Device Development
- Device Updates
- Vehicle Updates

**Certificate Authority for Security**

- Green=Policy team
- Blue=SE team
- Pink=Outreach/Comm
- Gold=Model Deployment
C. RISK ALLOCATION / DATA OWNERSHIP

The move to cooperative data systems complicates the issue of liability and where risk resides with the delivery of safety advisories and warnings. The issue is further complicated by the introduction of aftermarket devices, retrofitting of vehicles, and the risk of non-vehicle manufacturers accessing sensitive vehicle data.

The initial deployment of the basic safety message as part of the model deployment faces a limited set of liability challenges, which includes questions such as; how are vehicle or device manufacturers liable? Multiple sources of data and applications add complexity to the liability question, especially when data is developed in a cooperative manner. It is important to understand how risk is allocated among the many players that own the data and how one determines data ownership. Also, if NHTSA decides to issue a regulation for use of DSRC for safety, legal research will be needed to determine whether the basic safety messages and messages from applications can be covered under existing Federal liability statutes. The purpose of this policy area is to evaluate these issues in support of a clear understanding of data ownership rules and risk allocation.

1. Policy Questions

Risk Allocation

- How will risk be allocated when collisions occur in a V2V environment using cooperatively produced data?
- 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 a regulatory decision is made, do existing liability laws cover these situations? If so, what is the role of the Federal government in exercising this authority for daily operations? What role do state and local laws play?
- How does liability change in instances where there is negligence in properly maintaining in-vehicle systems? How does driver behavior or negligence (shutting off in-vehicle systems) change liability?

Data Ownership

- What are the rules and criteria in determining data ownership? Who can use data and for what purposes? How would proper use be managed and controlled?
- What types of responsibilities and/or rights come with data ownership?
- Are there different data ownership rights/rules between data senders and data receivers?
- When data passes through an algorithm that enhances the data and does ownership change as a result?
- What data from the vehicle is made available to aftermarket devices? What data should be made available and how does this shift risk allocation and liability?
- How should data from the vehicle be made available to aftermarket devices that ensure safe and reliable vehicle operations?
- How will IP rights be addressed? Are there examples in other modes that can provide insight (transit?)
- How can IntelliDrive leverage the value of data its system generates?
- What is the chain of ownership (of data) in a crash scenario?
2. **Research Tasks**

- Identify difference between proprietary and non-proprietary data that would be used in basic safety message and applications. Clearly differentiate between common (‘open source’) and proprietary algorithms in basic safety messages and identify where cooperative systems change the nature of data ownership. (For V2V and V2I).

- Engage legal experts to assess existing data ownership laws and practices. In particular, identify:
  - Cases involving transit data ownership and other current examples.
  - Ownership of data that resides on the vehicle.
  - Vehicle “Black Box” access and ownership laws and issues.

- Engage legal experts to identify liability issues associated with V2V and V2I systems, including:
  - Liability conventions for conventional traffic control devices and signal systems.
  - Existing government immunities similar to FAA systems or emergency systems.
  - Review of state laws and immunities.

- 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 devices and equipment) for V2V and V2I for spot safety using both embedded devices and aftermarket devices. Analyze impact to market opportunities.

- Collaborate with the insurance industry to determine broader industry impacts and concerns they might have with potential risk allocation models.

- Coordinate with IntelliDrive Data Capture Research Program to share information on data ownership issues.

3. **Stakeholder Collaboration:**

The following stakeholders are considered full participants and are directly engaged in research tasks and development:

- **Federal Government:** Will identify issues that need further analysis and support engagement with content experts. Stakeholders include ITS JPO, NHTSA, FHWA, FMCSA, FTA.

- **Legal (Technology) Firms and Trial Lawyers:** Will assess existing laws and practices and apply to V2V and V2I environment. Will help identify whether existing government immunities and conventions for traffic control devices apply. Will work collaboratively with research team to develop a risk allocation/liability model with identification of data ownership issues.

- **Vehicle Manufacturers and Device and Equipment Manufacturers:** Will provide information on existing laws and practices from their legal teams as well as desired outcomes of the risk allocation/liability model. Will be engaged throughout the process to comment on the risk allocation model as it develops and provide information on industry impacts. Stakeholders to be engaged directly and through CAMP, VIIC, SAE, ITS America, SEMA, CEA.

- **State and Local Governments and Local transportation agencies:** Will provide input on efficacy of existing laws and practices with conventional traffic control devices. Will be engaged on issues of data ownership and throughout the process to review options for IntelliDrive safety
risk/liability allocation and data ownership analysis. Stakeholders to be engaged through AASHTO, ITE, APTA, IBTTA and others as needed.

- **Universities/Evaluation Community**: Will provide insights on relevant past and existing experiences and lessons learned. Stakeholders to be engaged through university outreach networks, IntelliDrive knowledge management tool, meetings or projects.

- **Data Providers**: Will provide input on existing practices on data collection, processing, and selling. Will be engaged throughout the process.

4. **Stakeholder Outreach and Education:**
   The following stakeholders are indirectly engaged in research development and tasks and will act as informational resources. Ongoing education and outreach of research activities will be communicated with these stakeholders.

   - **Insurance Associations and Firms**: Will be engaged in providing inputs to the risk allocation model. They can provide information on how the risk allocation/liability model impacts existing models for the insurance industry and broader insurance market.

   - **Legal Firms and Trial Lawyers**

5. **Outcomes for Safety Pilot:**
   - Initial data ownership and management model.

6. **Outcomes for NHTSA Regulatory Decision:**
   - An initial model outlining possible risk allocation schemes.
   - Analysis of data ownership and management plan, outlining benefits and industry impacts.
   - Assessment of intellectual property and patent issues.
   - A legal assessment of government immunities and relevant case examples relevant for the V2V environment.

7. **Outcomes for Deployment:**
   - Determination on whether new legislation is necessary for immunity and for assigning or limiting liability (if appropriate).
   - Data ownership and access models.
   - Potential incorporation of new immunities (if appropriate) as part of regulation.
   - Guidelines for built-in, retrofit, and aftermarket IntelliDrive devices with respect to data and liability.

8. **Roadmap**

   Research activities in this roadmap will be closely coordinated with research for the Dynamic Mobility Applications and Data Capture program, as many of these policy issues are relevant across all of these areas.
The figure outlines a timeline and process for Risk Allocation and Data Ownership, with key milestones and activities scheduled for CY 2010 to CY 2013.

**Risk Allocation and Data Ownership**

- **CY 2010**: Q1-Q4
  - Model Deployment: Ramp-up and Preliminary Testing
  - Stakeholder outreach and education

- **CY 2011**: Q1-Q4
  - Identify data types and ownership issues
  - Evaluate data ownership laws and practices
  - Develop Risk Allocation/Data Ownership Model
  - Engage risk allocation (insurance industry, etc.) experts
  - Market Analysis on impact of risk and liability issues

- **CY 2012**: Q1-Q4
  - Model Deployment: Full-Scale Testing
  - Input to industry standards based upon test results
  - Modify Risk Allocation/Data Ownership Model
  - V2V Regulatory Decision Point

- **CY 2013**: Q1-Q4
  - Aftermarket Device Development
  - Device Updates
  - Vehicle Updates
  - V2V Benefits Assessment
  - Working Group Review

Key activities include:

- Model Deployment
- Stakeholder outreach and education
- Identifying data types and ownership issues
- Evaluating data ownership laws and practices
- Developing Risk Allocation/Data Ownership Model
- Engaging legal and risk allocation experts
- Market analysis on the impact of risk and liability issues
- Input to industry standards based upon test results
- Modifying Risk Allocation/Data Ownership Model
- V2V Regulatory Decision Point
- Aftermarket Device Development
- Device updates
- Vehicle updates
- V2V Benefits Assessment
- Working Group Review

The timeline is color-coded with Green for Policy team, Blue for SE team, Pink for Outreach/Comm, and Gold for Model Deployment milestones and review points.
D. Cost-Benefit Assessment in Support of Deployment

Cost-Benefit analysis (CBA) is a critical tool in developing the basis for a regulatory decision. In order to support an evidence-based decision, a rigorous cost-benefit analysis of the V2V and V2I Safety applications will be conducted. The cost benefit analysis will include quantitative analyses of associated costs (vehicle equipment, retrofitting, RSEs) and benefits (crash avoidance, safety).

1. Policy Questions

- What assumptions will be used in calculating the costs and benefits of vehicle safety communications?
- What vehicle classes (passenger, commercial, transit vehicles, etc.) are to be included in the cost benefit analysis?
- What cost benefit data is necessary for supporting the regulatory decision process?
- How effective is V2V and V2I technology at reducing crashes? What technology if any needs to be mandated to obtain benefits, with respect to both vehicle to vehicle and vehicle to infrastructure communications?
- What are likely deployment scenarios and timeframes will be used in the cost benefit analysis? What are potential development and operating costs of any governance/oversight/operational entities needed?
- What type of benefits are V2V and V2I Safety applications expected to produce and what should be included in the cost/benefit analysis?
- 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?
- How will the cost of mandating 5.9GHz DSRC for V2V and V2I Safety impact the nation? Agencies? Manufacturers? Citizens?
- How do you incorporate retrofit and aftermarket equipment into the CBA? How does this affect the underlying assumptions around the vehicle fleet penetration model?
- If V2V and V2I Safety followed a phased-in approach, how will the cost/benefits change over time? How will it reflect greater vehicle fleet penetration?
- How does the Cost/Benefit analysis change based on installation type (OEM equipment, retrofit, and aftermarket install)?

2. Research Tasks

- Collaborate with V2V Safety technical research team to develop assumptions and constraints for CBA model.
- Validate CBA model with public working group including stakeholders (OEMs, state and local transportation agencies).
- Analyze specific applications 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.
- Determine the feasibility and value proposition for retrofit and aftermarket devices.
- Incorporate any relevant input or outcomes from the Safety Pilot into the CBA analysis.
- Work with NHTSA office for rulemaking to develop a process and timeline for gathering data in support of the regulatory decision.
• Determine potential costs or benefits using varying certification and CA structures, including the application of standards, risk allocation and data ownership models.
• Provide assessment of industry impacts and on specific stakeholder groups. This task should include an economic impact analysis to agencies, manufacturers, citizens and others.
• Coordinate with NHTSA to provide appropriate data inputs necessary for the regulatory decision.

3. **Stakeholder Collaboration:**
The following stakeholders are considered full participants and are directly engaged in research tasks and development:

- **Federal Government:** Will develop the CBA model. Will also collaborate with industry and State and local agencies on developing model, assumptions, constraints, costs, and benefits.
- **Private Industry:** Will provide data inputs to the process. Potential stakeholders include OEMs, manufacturers of roadside equipment and communications technology developers.
- **Transportation Agencies:** Will provide data inputs to the process based on what vehicle classes are included in the mandate.

4. **Outcomes for Safety Pilot:**
- Cost-benefit and cost-effectiveness models established (assumptions, constraints, and initial costs) and validated with stakeholders.
- Preliminary evaluation on the data elements needed for the CBA and which could be produced from the Safety Pilot.

5. **Outcomes for NHTSA Regulatory Decision:**
- Cost benefit inputs for future NHTSA analysis.
- Agency, industry, citizen economic impact analysis.

6. **Outcomes for Deployment**
- Understanding of potential costs and benefits for deployment of V2V and V2I Safety applications.

7. **Roadmap**
### Cost-Benefit Analysis

**CY 2010**
- Q1: Collaborate with stakeholders to develop initial CBA model
- Q2: Review CBA model with public working group
- Q3: Conduct cost-effectiveness analysis on V2V applications, includes comparison to alternatives.
- Q4: Conduct industry impact analysis

**CY 2011**
- Q1: Collaborate with NHTSA to determine timeline and necessary data for regulatory decision
- Q2: Modify CBA model
- Q3: Incorporate relevant outcomes and data from Safety Pilot
- Q4: Finalize CBA

**CY 2012**
- Q1: Input to Industry standards based upon test results
- Q2: V2V Regulatory Decision Point
- Q3: Model Deployment Assessment
- Q4: Model Deployment Full Scale Testing

**CY 2013**
- Q1: Data-Based Policy Recommendation to NHTSA
- Q2: V2V Regulatory Decision Point

---

**Model Deployment**
- Aftermarket Device Development
- Device Updates
- Vehicle Updates
- Model Deployment Ramp-up and Preliminary Testing
- Model Deployment Full Scale Testing

---

**Cybersecurity**
- Input to Industry standards based upon test results

---

**V2V Benefits**
- Assessment
E. RULES OF OPERATION AND STANDARDS

IntelliDrive represents a nationwide system covering multiple states and jurisdictions. In addition, there will be multiple users of the system that represent a wide variety of public and private sector entities. The sheer complexity of the system emphasizes the need for establishing a set of rules of use and operation, as well as rules for the application of standards. The purpose of this policy area is to ensure that all participants of the IntelliDrive system follow a common set of rules and standards that will ensure interoperability, effectiveness, and protection of the users and providers of the IntelliDrive system.

1. Policy Questions

Rules of Use and Operation:

- What will be the rules of use and operation, according to federal, state, and local laws (jurisdictions)?
- 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?
- Is it possible for any of the rules to have flexibility to tailor to local needs? If so, which ones?
- Are there specific rules for OEMs, aftermarket equipment suppliers, or others? Who are the others?
- 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?
- What rules are needed to ensure safe and efficient operations of the system across multiple vehicle manufacturers and for in–vehicle hardware suppliers? Who will design, test and enforce these rules?
- Who will monitor for misbehavior or misuse of the system?
- Who will have access to the system? Are there certain entities that will not be allowed to have access?
- Will different components of the system require varying levels of access? If so, what are the components and access levels? (e.g. hardware, software, communications infrastructure)
- How will rules of operation and use be administered and enforced?
- How will disputes be handled? Will a separate entity be involved or will this default to the current legal system?

Standards:

- Which entities will issue standards?
- Who will enforce use of standards? Is a 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?
- Is an official entity needed to set 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 of competing standards?
- Will only certified device systems have access to the 5.9GHz spectrum?
• What are the appropriate roles of the Federal government, transportation agencies, and industry in developing standards?
• 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?
• How will the problem of basic signal equipment maintenance and upkeep be integrated into technical standards, such as minimum acceptance availability rates?

**Enforcement:**
• What aspects of the system require enforcement?
• How will enforcement be conducted for different components of the system, for example, vehicle equipment, communications infrastructure, and aftermarket equipment?
• 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 criminal prosecution of fraudulent messages? How? Does this violate privacy principles?
• 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?

2. Research Tasks

**Rules of Use and Operation**
• 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 (e.g. internet).
• Engage stakeholders to develop potential rules of use and operations, including identifying user groups, required authorities, and technical needs.
• Develop a preliminary assessment of operational requirements, additional costs and institutional issues.
• In alignment with activities under the governance policy area, identify who will have the authority to develop and enforce rules of operations and use of standards.

**Application of Standards**
• Conduct an evaluation of existing device and equipment certification processes (see Section A.) to ensure that they appropriately address the application of standards.
• Determine appropriate roles and responsibilities in standards setting, including the Federal role.
• Pursue international harmonization of standards.
• Engage legal experts to assist in categorizing “illegal” or “misuse” behavior.

**Enforcement**
Partner with system developers and security experts in order to determine whether mechanisms can be built into the system to identify misuse and to address misbehavior. This activity should also include a ‘concept of operations’ outlining different security scenarios.

- Identify appropriate and feasible enforcement mechanisms and evaluate whether these mechanisms violate privacy principles.
- Analyze State and local legislation to determine if new laws will be in conflict or if existing laws prohibit enforcement.
- Conduct an assessment of enforcement requirements, including identifying need for different levels of enforcement.

3. **Stakeholder Collaboration:**
The following stakeholders are considered full participants and are directly engaged in research tasks and development:

- **Federal Government:** Will facilitate stakeholder engagement on rules of operations, requirements for enforcement, and toolbox of enforcement techniques.
- **Systems Developers:** Will provide input in determining enforcement mechanisms and its impact on privacy.
- **Privacy Advocates:** Will provide input on privacy requirements, specifically on balancing the need for system enforcement and protecting privacy.
- **Transportation Agencies, Manufacturers, Industry:** Will be engaged in setting requirements for rules of operations.
- **Standards Development Organizations:** Will help define roles and responsibilities in standards setting.
- **International Standards Organization:** Will facilitate international harmonization.

4. **Outcomes for Safety Pilot:**
- A potential set of rules of use and operations designed to be used during the Safety Pilot.
- A series of security scenarios that can be introduced during the Safety Pilot as a way to test select enforcement techniques.

5. **Outcomes for NHTSA Regulatory Decision:**
- Recommended rules of operation to be used as an input into the NHTSA regulatory decision.

6. **Outcomes for Deployment:**
- Potential set of rules of operations and standards for deployment.
- Recommended plan towards achieving harmonization of standards (including international standards).
- Recommended enforcement mechanisms and an analysis on the need for new legislation regarding enforcement.

7. **Roadmap**
Rules of Operation and Standards

<table>
<thead>
<tr>
<th>CY 2010</th>
<th>CY 2011</th>
<th>CY 2012</th>
<th>CY 2013</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q1</td>
<td>Q2</td>
<td>Q3</td>
<td>Q4</td>
</tr>
</tbody>
</table>

- **Stakeholder outreach and education**
- **Review rules of ops for other systems**
- **Engage stakeholders and experts**
- **Develop Preliminary Assessment (enforcement, standards, operational requirements)**
- **Analysis of state and local legislative issues**
- **Determine roles and responsibilities**
- **Determine roles and responsibilities**
- **Analysis of international harmonization of standards**
- **Recommended Rules of Operation**

**Model Deployment**
- **Aftermarket Device Development**
- **Device Updates**
- **Vehicle Updates**
- **Model Deployment: Ramp-up and Preliminary Testing**
- **Model Deployment: Full Scale Testing**
- **V2V Regulatory Decision Point**
- **Input to Industry standards based upon test results**
- **V2V Benefits Assessment**
F. SPECTRUM ANALYSIS AND FCC ROLE

The IntelliDrive 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 (or have access). The purpose of this policy area is to evaluate the role of a spectrum manager (if necessary) and to identify issues relevant to spectrum use.

1. Policy Questions

- Will V2V and V2I Safety require the use of a ‘spectrum manager’? If so, who are potential candidates for this role?
- What are the roles and responsibilities for spectrum management?
- How does the role of a spectrum manager interact/overlap with CA?
- What restrictions will be applied in allowing entities to use the spectrum? More specifically, how will ‘safety’ be defined in limiting spectrum access to ‘safety’ applications only?
- Are there international issues relevant to spectrum use?
- How will the definition of a governance entity 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?

2. Research Tasks

- Develop an assessment of the current process by which the FCC currently regulates spectrum use and identify issues unique to IntelliDrive.
- Conduct an analysis on the existing process to determine whether a different process needs to be established for IntelliDrive.
- Conduct an analysis on past or current examples of spectrum management and FCC regulation that could provide lessons learned for IntelliDrive.
- Evaluate other interagency arrangements regarding FCC spectrum regulation, some examples include the FBI.
- Determine whether and how a research or experimental license can be used for testing.
- In collaboration with stakeholders, define the requirements, roles and responsibilities for using a spectrum manager and determine which entities meet the requirements.
- Evaluate potential entities that could operate as a spectrum manager and define evaluation criteria that could be used to select a spectrum manager.
- Coordinate with the FCC on spectrum use and begin development of plans for V2V and V2I Safety.
- Discuss the processes in place for FCC to assure valid use and non-interference.
- Determine whether there is a need for developing licensing guidelines for users.

3. Stakeholder Collaboration:

The following stakeholders are considered full participants and are directly engaged in research tasks and development:
• **FHWA**: Will provide input on existing licensing process.
• **FCC**: Will provide input on policy questions and on appropriate FCC roles and responsibilities.
• **NTIA**: Will be involved in addressing domestic and international telecommunications and information policy activities.
• **Vehicle manufacturers and fleet owners/operators, transportation agencies, device and equipment manufacturers**: Will provide input on spectrum manager requirements, roles, and responsibilities.

4. **Outcomes for Safety Pilot**:
   • Preliminary understanding of existing FCC processes and current spectrum regulation practices.
   • Appropriate licensing for conducting Safety Pilot research (experimental license)

5. **Outcomes for NHTSA Regulatory Decision**
   • Recommendation on the need and role of a spectrum manager. This will also include an analysis on multiple options available regarding spectrum management.
   • Recommendations and input on potential FCC role and responsibilities relevant for IntelliDrive.

6. **Outcomes for Deployment**
   • Potential design of roles and responsibilities for spectrum management.

7. **Roadmap**
G. INFRASTRUCTURE (V2V AND V2I SAFETY)

Both V2V and V2I Safety will include some level of roadside communications infrastructure. For V2V Safety, roadside infrastructure may be used for authenticating certificates and for ensuring system security. For V2I Safety, roadside infrastructure is a key component for providing safety applications. Deployment, maintenance, operations, and financing of roadside infrastructure represent a few of the key issues under this policy area. The purpose of this area is to identify key needs for infrastructure and to determine how the maintenance, operations, financing, and oversight of infrastructure will be met.

1. Policy Questions

Needs, Roles and Responsibilities

- What are the range of roles for the public sector in the installation, operation and maintenance of RSEs? What about the private sector?
- How do we leverage existing systems for infrastructure/roadside equipment? What are specific infrastructure needs?
- What is the acceleration of safety, mobility, and other benefits due to infrastructure deployment?

Maintenance and Operations

- Who will be responsible for setting up and maintaining the required roadside equipment?
- Who will be responsible for setting up and maintaining the required connections from the roadside equipment to the certificate authority?
- How will replacement cycles for roadside equipment be established?
- How will staffing needs and training be addressed at deployment agencies (e.g. 5.9GHz training)?

Financing

- What are the estimated costs for deploying, operating and maintaining an RSE? What are the potential business models for supporting these costs?
- How will the hardware, installation, maintenance, and replacement of equipment be financed?
- Is it possible to use a Public-Private-Partnership model in deploying and financing roadside communications infrastructure?
- What is needed to mandate RSE placement for spot safety for an FHWA rule? What can be done to enforce that rule in an era where funds for existing programs are already insufficient?

2. Research Tasks

- Conduct evaluation to determine the minimum level of roadside infrastructure necessary. In this evaluation, address the tradeoff between level of infrastructure and security.
- Develop an assessment on potential design and feasibility of infrastructure, including cost estimates and placement.
• Engage AASHTO, local transportation authorities, and other key stakeholders to identify issues with roadside equipment and operations and maintenance.
• Evaluate technology upgrades and continuing maintenance of infrastructure
• Determine the staffing requirements for installing and maintaining roadside equipment.

3. Stakeholder Collaboration:
The following stakeholders are considered full participants and are directly engaged in research tasks and development:

• **Federal Government:** Will lead stakeholder engagement and provide input on infrastructure requirements.
• **Transportation Agencies:** Will provide input on infrastructure maintenance, operations, deployment, and funding.
• **Vehicle Manufacturers and Security Experts:** Will provide input on the level of infrastructure needed for security and certificate authority purposes.
• **Traffic signal control manufacturers:** Will provide input on how these devices can be incorporated into existing traffic signal control hardware to minimize the addition of new devices in the field. (ITE, IMSA)
• **Tolling Industry (owner/operators and tolling hardware suppliers):** Will provide input on existing infrastructure systems and potential synergies with IntelliDrive system (IBTTA).

4. Outcomes for Safety Pilot:
• Preliminary configuration of roadside infrastructure to be tested during the Safety Pilot, where the infrastructure addresses certificate authentication.
• Preliminary configuration of roadside infrastructure to be tested during the Safety Pilot, where V2I Safety applications will be tested.

5. Outcomes for NHTSA Regulatory Decision:
• Initial recommendations and input on the minimum level of roadside infrastructure necessary for V2V Safety, which will provide input to the regulatory decision.

6. Outcomes for Deployment:
• Guidance on potential funding, deployment and maintenance options for V2V and V2I Safety roadside infrastructure.

7. Roadmap
Infrastructure for V2V and V2I Safety

**CY 2010**

- Q1: Initial Evaluation
- Q2: Infrastructure Needs

**CY 2011**

- Q1: Feasibility Assessment of Infrastructure Design & Cost
- Q2: Determine staffing needs for maintenance and operations
- Q3: Feasibility Assessment of Infrastructure Design & Cost
- Q4: Determine staffing needs for maintenance and operations

**CY 2012**

- Q1: Infrastructure Needs Defined
- Q2: Stakeholder outreach and education
- Q3: Stakeholder outreach and education
- Q4: Engage key stakeholders for input and review

**CY 2013**

- Q1: Developed recommended process for technology upgrades and maintenance
- Q2: Recommended level of infrastructure needs and O&M process
- Q3: Input to Industry standards based upon test results
- Q4: V2V Regulatory Decision Point

---

### Model Deployment

- Aftermarket Device Development
- Device Updates
- Vehicle Updates
- Model Deployment Ramp-up and Preliminary Testing
- Model Deployment Full Scale Testing

### V2V Benefits Assessment

- V2V Regulatory Decision Point
H. GOVERNANCE STRUCTURE AND AUTHORITY

A governance structure is necessary for framing the roles, responsibilities, and authorities of participants of the IntelliDrive system. Findings from previous policy areas (Sections A-G) will help inform the issue of governance and provide the framework for developing a governance structure. The issue of governance represents a broader and global policy area. The purpose of this area is to leverage the research performed under the previous policy areas as a foundation for developing a feasible governance structure and authority.

1. Policy Questions
   - Is a governance structure necessary? What aspects of IntelliDrive require governance (as distinct from those aspects that can be left to the private sector)?
   - How many governing bodies are necessary, one or multiple?
   - What type of governance entity is appropriate? Should it be a Federal, state, local, or private sector entity or both?
   - Is a regional governance model or multi-state model possible?
   - Are new authorities necessary for governance?
   - What type of entity will be most effective for oversight, operations, and enforcement?
   - How will a governance entity or entities balance competing needs? Resolve conflicts?
   - 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?
   - Will different participants of the IntelliDrive system require separate governance entities? For example, public transportation agencies, retrofit equipment manufacturers, OEMs, etc.?
   - What are operational requirements for governance entities?
   - What are estimated costs for establishing and operating governance entities?

2. Research Tasks
   - Conduct an assessment of existing governance structures that could be similar or could provide best practices for IntelliDrive. This assessment should include a range of models, such as government and industry partnerships, industry led organizations, and government led initiatives.
   - Identify governance experts. In collaboration with experts, develop a potential governance model that addresses key policy issues from previous sections, such as; a) enforcement, b) rules of operations, c) standards, d) security, e) risk allocation, and f) and privacy, as well as others.
   - Hold a governance workshop to engage stakeholders and to elicit feedback on potential governance model.
   - Revise governance model based on feedback received during governance workshop.

3. Stakeholder Collaboration:
   The following stakeholders are considered full participants and are directly engaged in research tasks and development:
- **Federal Government**: Will coordinate the research, engage experts, and facilitate dialogue among the governmental and industry players that will be impacted by the governance structure.
- **State and Local Transportation Agencies**: Will provide input on governance needs.
- **Vehicle manufacturers and suppliers**: Will provide input on governance needs.
- **Governance Experts**: Will provide input on existing examples of governance and give expert advice on potential governance structures for IntelliDrive.

4. **Outcomes for Safety Pilot**:
   - None

5. **Outcomes for NHTSA Regulatory Decision**:
   - Recommended governance structure in support of V2V and V2I for spot safety, outlining suggested roles and responsibilities.

6. **Outcomes for Deployment**:
   - Recommended governance entity with associated operations, roles, responsibilities, and capabilities.

7. **Roadmap**

   **Governance Structure & Authority**

   **CY 2010**
   - Q1: Stakeholder outreach and education
   - Q2: Assess Governance Needs and Existing Examples
   - Q3: Develop Initial Governance Model
   - Q4: Modify Governance Model

   **CY 2011**
   - Q1: Engage Governance Experts
   - Q2: Develop Implementation strategy for governance model
   - Q3: Working Group Governance Workshop
   - Q4: Final Draft V2V Governance Model

   **CY 2012**
   - Q1: Aftermarket Device Development
   - Q2: Device Updates
   - Q3: Vehicle Updates
   - Q4: V2V Regulatory Decision Point

   **CY 2013**
   - Q1: Model Deployment Ramp-up and Preliminary Testing
   - Q2: Model Deployment Full Scale Testing
   - Q3: Input to Industry standards based upon test results
   - Q4: V2V Benefits Assessment