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

Identification of Critical Policy Issues for the Mobility Program

www.its.dot.gov/index.htm

FINAL REPORT — May 2012
FHWA-JPO-12-035

Produced by the John A. Volpe National Transportation Systems Center
U.S. Department of Transportation
Research and Innovative Technology Administration
ITS Joint Program Office

Notice

Acknowledgements

The Volpe Center team would like to acknowledge the leadership of Walter During, P.E., of the Office of Transportation Management (HOTM) within the Office of Operations, Federal Highway Administration, U.S. Department of Transportation, in providing the guidance necessary to review the Connected Vehicle Environment Mobility Program's systems, technologies, and applications to identify the critical policy and institutional issues and produce this document.

Technical Report Documentation Page

1. Report No.	2. Government Accession No.	3. Recipient's Catalog No.
FHWA-JPO-12-035		

4. Title and Subtitle	5. Report Date
Identification of Critical Policy Issues for the Mobility Program	May 2012
	6. Performing Organization Code

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. Performing Organization Report No.
Ingrid Bartinique, Josh Hassol, Deirdre Herring, Amy Sheridan, Suzanne Sloan, and Dicky Waldron	

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. Work Unit No. (TRAIS)
U.S. Department of Transportation Research and Innovative Technology Administration John A. Volpe National Transportation Systems Center 55 Broadway Cambridge, MA 02142	11. Contract or Grant No. HW4A3

12. Sponsoring Agency Name and Address	13. Type of Report and Period Covered
U.S. Department of Transportation Federal Highway Administration (FHWA) Office of Advanced Travel Management (HOTM) 1200 New Jersey Ave., S.E. Washington, D.C. 20590	Policy Analysis, 2011-2012
	14. Sponsoring Agency Code

15. Supplementary Notes

16. Abstract

The intent of this white paper is to identify and describe critical policy and institutional challenges that are anticipated with:

- Development and operations of new connected vehicle data capture and management (DCM) technologies and systems
- New systems for developing open source applications
- Development and commercialization of the new connected vehicle dynamic mobility applications (DMA)

It is the intention of the research programs that are guiding these efforts to implement open data and open source policies, to the extent feasible, as a means of supporting the public sector with less costly technologies as well as to encourage more dynamic market innovation. The USDOT's interest in implementing open data and open source policies is reflective of a broader Federal effort to support the *Open Government Directive* which is focused on promoting the principles of transparency, participation, and collaboration with citizens to achieve greater involvement in government.

Implementing DCM and DMA based on open data and open source policies may present critical challenges during the research stages of concept development, prototyping, and testing; and present obstacles to technology transfer, market adoption, and commercial operations. The challenges (or critical issues) described in this white paper are a result of a preliminary analysis of the emerging DCM and DMA systems, technologies, and applications; a review of the technical, evolutionary path for both programs; and a review of Federal, State and local, academic, and commercial practices (documented in a separate white paper).

17. Key Words	18. Distribution Statement
Open data and open data environments, open source portals, dynamic mobility applications, Core System, privacy, liability, user access controls, metadata, standards, user registration, project forking, governance, intellectual property, data capture and management, policy and institutional issues, policy analysis, policy recommendations	

19. Security Classif. (of this report)	20. Security Classif. (of this page)	21. No. of Pages	22. Price
None	None	50	

Table of Contents

List of Tables

Executive Summary

The Federal Highway Administration (FHWA), in partnerships with the Intelligent Transportation Systems (ITS) Joint Program Office (JPO), the Federal Transit Administration (FTA), the National Highway Traffic Safety Administration (NHTSA), and the Federal Motor Carrier Safety Administration (FMCSA) are working to research, develop, and facilitate adoption of the next generation of advanced transportation technologies and systems related to mobility and operations. The focus of the current research is on the transformative nature of wireless technologies that create connectivity between vehicles, between vehicles and roadway infrastructure, and with mobile devices—known as the connected vehicle environment. If the connected vehicle technologies prove to be truly transformative, they will significantly reduce safety problems, enhance mobility, and reduce the environmental impact that transportation has on the environment.

From the perspective of enhancing mobility, the connected vehicle technologies are expected to generate a higher volume and better quality of data through new sources of vehicle-based data. Using these new data sources to populate open data environments, public sector agencies, private sector firms, and consumers will have access to multi-source, real-time data for synthesis into dynamic mobility applications.

Purpose of this White Paper

This white paper describes the critical policy and institutional issues associated with applying open data and open source policies to connected vehicle systems, technologies, and applications for mobility, specifically during:

- Development, testing, and demonstration phases of new, connected vehicle data capture and management (DCM) technologies, datasets, and systems
- Development, testing, and operations of a new open source applications development portal (OSADP)
- Development and commercialization of new dynamic mobility applications (DMAs).

The U.S. Department of Transportation's (US DOT) Data Capture and Management (DCM) and Dynamic Mobility Applications (DMA) programs have envisioned implementing open data and open source policies as a means of:

- Supporting public sector needs with less costly technologies
- Promoting collaboration and innovation
- Encouraging new market opportunities

Four primary elements of the DMA and DCM programs are considered within this white paper:

1. The DCM program's open datasets

2. The DCM program's open data environments – a Prototype Data Environment (PDE), a Research Data Exchange (RDE), and envisioned operational environments
3. The DMA programs Open Source Applications Development Portal (OSADP)
4. The DMA program's dynamic mobility applications (DMAs).

Implementing DCM and DMA based on open data and open source policies are expected to present critical challenges during the research stages of concept development, prototyping, and testing; and present obstacles to technology transfer, market adoption, and commercial operations. The challenges (or critical issues) described in this white paper are a result of a preliminary analysis of the emerging DCM and DMA systems, technologies, and applications; a review of the technical, evolutionary path for both programs; and a review of Federal, State and local, academic, and commercial practices (documented in a separate white paper).

In addition to identifying and describing the critical issues that are most likely to occur, this white paper also establishes the parameters and focus of future research that will result in policy recommendations.

Structure of this White Paper

This white paper is divided into chapters that explore and describe the critical issues associated with each DCM or DMA technology, system, or set of applications as follows:

- Each chapter begins with a definition and presentation of a chart that lists the critical issues specific to the technology, system, or application on the left side and the stages of research through commercialization on the right side. The result is to provide the reader with an overall summary of the content to be discussed within the chapter.
- A following table identifies when the critical issues may have the most impact (and thus require options and recommendations for resolution) during the technical stages. In providing this second table, the technical research team has a roadmap that helps prioritize when policy and institutional issues will need to be addressed.
- The remainder of each chapter offers a definition of each critical issue and lists the questions as a means of guiding the focus of policy research and analysis (whose results will be documented in a series of upcoming reports). The chapters include:
    - Chapter 1: Critical Policy Issues for Implementing Open Data and for Prototype, Research, and Operational Data Environments
    - Chapter 2: Critical Policy Issues with the Development and Operations of an Open Source Portal
    - Chapter 3: Critical Policy Issues with the Development of New Dynamic Mobility Applications
    - Chapter 4: Critical Policy Issues with Core System Integration

Mobility Policy Analysis Reports

This report is one in a series of six policy reports that describe and analyze the policy issues associated with connected vehicle mobility. The series includes:

- Two foundational reports that identify the critical issues and describe the best practices and lessons learned from government, industry, and academia:
    - ***Identification of Critical Policy Issues for the Mobility Program*** (this report), FHWA-JPO-12-035
    - ***State-of-the-Practice and Lessons Learned on Implementing Open Data and Open Source Policies*** FHWA-JPO-12-030

- Four reports that analyze the specific policy issues in context of the goals of the DMA and DCM programs:
    - ***Policy Analysis and Recommendations for the Open Source Applications Development Portal (OSADP)***, FHWA-JPO-12-031
    - ***Policy Analysis and Recommendations for Development of the Dynamic Mobility Applications***, FHWA-JPO-12-033
    - ***Policy Analysis and Recommendations for the DCM Research Data Exchange***, FHWA-JPO-12-036
    - ***Privacy and Security Analysis and Recommendations for the DCM and DMA Programs***, FHWA-JPO-12-032

Recommendations for Policy Research

The following tables summarize the recommendations for policy research. The four tables reflect the results of each chapter. The tables present three columns of information:

1. The policy issues are identified in Column A.
2. The expected outcomes from pursuing policy research are identified in Column B.
3. The name of the report or reports that will include the research and analysis is in Column C.

Table ES 1: Research Recommendations for Open Data and Data Environment Policies

(A) Critical Issues	(B) Expected Outcomes from Policy Research	(C) Policy Reports
• **Governance/ Data Governance Policies**	• *Identification of needs for governance and authority* • *Analysis of whether new authorities are needed* • *Definition of roles and responsibilities* • *Identification of options for policies on federation, data sharing, and maintenance of data environments.* • *RESULT:* o *Recommended governance policies for Data Environment/Exchanges and data governance* o *Recommended next steps in developing protocols and procedures.*	Options are identified in the report: ***State-of-the-Practice and Lessons Learned on Implementing Open Data and Open Source Policies.*** The following reports will analyze all of the policy requirements, present recommended policies, and identify next steps. • ***Policy Analysis and Recommendations for Open Source Application Development Portal*** • ***Policy and Recommendations for the DCM Data Exchange***
• **Data Environment Policies / System Rules of Operation**	• *Analysis of risk and identification of policy options that address technologies and design, user access and control policies, security, metadata, data quality assurance, rules of conduct, enforcement and monitoring, language policy, and application of standards.* • *RESULT:* o *Policy recommendations and proposed system rules of operation.*	
• **Liability / Risk Mitigation Strategies**	• *Identification of liability risks and identification of new liabilities introduced by connected vehicle data capture and management and open data.* • *RESULT:* o *Risk mitigation policy recommendations.*	
• **Intellectual Property Policies**	• *Analysis on intellectual property risks associated with the open data exchanges (RDE) and the data sets.* • *RESULT:* o *Policy recommendations to protect intellectual property.*	
• **Privacy / Data Usage Policies**	• *Privacy analysis for the datasets and the RDE regarding use of Personally-identifiable information (PII).* • *RESULT:* o *Initial application of the Fair Information Practices (FIPs).*	Privacy and security are addressed in a report titled: ***Privacy and Security Analysis and Recommendations for the DCM and DMA Programs.***

Table ES 1: Research Recommendations for Open Data and Data Environment Policies (continued)

(A) Critical Issues	(B) Expected Outcomes from Policy Research	(C) Policy Reports
• **Business Models / Data Ownership Policies**	• *Analysis and options for data ownership.* • *Market research to identify the potential value of the new, vehicle-based data and comparison against the costs of capturing and managing it in a secured environment.* • *Market adoption/commercialization of the data environments.* • *RESULT:* o *Options for new business models/partnerships based on analysis of the RDE's implementation, lessons learned, cost elements, and revenue options for financially sustaining data environments.*	The Legal Policy team is exploring data ownership policies and will inform the Mobility policy analysis process in the January/February 2012 timeframe. The Implementation Policy team is analyzing business models and researching the value of data and will inform the Mobility policy analysis process throughout spring 2012.
• **Application of Other Federal Policies**	• *Identifications and recommendations regarding other Federal policies that may be required for the datasets or the RDE* • *RESULT:* o *Recommendations on what Federal policies apply and analyses of the impacts.*	Results are documented in the report: ***State-of-the-Practice and Lessons Learned on Implementing Open Data and Open Source Policies.***

Table ES 2: Research Recommendations for the Open Source Applications Development Portal Policies

(A) Critical Issues	(B) Expected Outcomes from Policy Research	(C) Policy Reports
• **Program and Portal Governance Policies (Addresses System Governance for the Web-based portion of the portal and the community environments; also addresses system decision making and conflict resolution)**	• *Identification and analysis of options for OSADP program and portal-level governance.* • *Analysis of model effectiveness for achieving the DMA program goals for rapid, collaborative application development with transparency and the ability to retain rights for software licensing/ distribution to public agencies.* • *RESULT:* o *Recommended steps for implementation.*	Options are identified in the report: ***State-of-the-Practice and Lessons Learned on Implementing Open Data and Open Source Policies.*** A forthcoming research report titled: ***Policy Analysis and Recommendations for the Open Source Applications Development Portal (OSADP)*** will address governance. Security is also addressed in a report titled: ***Privacy and Security Analysis and Recommendations for the DCM and DMA Programs.***
• **Project Governance Policies (Addresses user controls and access policies for the Applications Development Environment and Applications Release Repository; also addresses rules of conduct)**	• *Identification and analysis of options for OSADP project-level governance (includes recommendations for management approach to projects, policy on collaboration and user access which further includes permissions/openness, user classes, rules of conduct, bundle versus application access policies, Project Forking policy, repository access policy, contributor recognition policy, and policy on use of standards).* • *RESULT:* o *Recommended steps for implementation.*	
• **Intellectual Property and Copyright/ Licensing and Liability**	• *Analysis on intellectual property associated with the dynamic mobility applications.* • *RESULT:* o *Policy options and recommendations.*	

Table ES 2: Research Recommendations for the Open Source Applications Development Portal Policies (continued)

(A) Critical Issues	(B) Expected Outcomes from Policy Research	(C) Policy Reports
• **DMA Development and Procurement Strategies**	• *Identification of risks associated with the development and procurement of the applications. Identification of implications for the OSADP.* • *RESULTS:* o *Recommended procurement and development strategies for achieving the DMA program goals for rapid, collaborative development and ability to retain rights with least amount of risk regarding intellectual property infringement, exposure of sensitive source code or data.*	A forthcoming research report titled: ***Policy Analysis and Recommendations for Development of the Dynamic Mobility Applications*** will address the impact that the choice of development and procurement may have the applications and the resulting implications for development within the OSADP. It will identify best practices in product liability mitigation. The Legal Policy team will be analyzing liability for the entire connected vehicle program and developing US DOT policy for addressing it.
• **Product Liability Issues**	• *Identification of risks and analysis on whether the new, dynamic mobility applications, in particular, those offered as free and open source software, introduces any new liabilities.* • *RESULT:* o *Recommended risk mitigation options.*	
• **OSADP Business Model**	• *Exploration of an OSADP business model for private sector or academic ownership and operations.* • *RESULT:* o *Framework for determining whether the OSADP might have post-research value.*	Analysis requires that the OSADP is defined and lessons gathered from operations before determining the potential value the OSADP might have to private sector or academic owners.

Table ES 3: Research Recommendations for the Dynamic Mobility Application Policies

(A) Critical Policies Issues	(B) Expected Outcomes from Policy Research	(C) Policy Reports
• **Development and Procurement Strategies**	• *Analysis of procurement options for each DMA application bundle.* • *RESULT:* o *Recommendation of appropriate development and procurement strategies for the applications.* o *Identification of implications for the OSADP design and operations.*	A forthcoming research report titled: ***Policy Analysis and Recommendations for Development of the Dynamic Mobility Applications*** will address the impact that the choice of development and procurement strategies may have on dynamic mobility applications and the implications for development within the OSADP.
• **Data Privacy**	• *Analysis of privacy requirements associated with each application and application bundle.* • *RESULT:* o *Initial application of the Fair Information Practices (FIPs).*	A forthcoming research report titled: ***Privacy Analysis and Recommendations for the DCM and DMA Programs*** will explore the privacy risks associated with the applications and identify mitigating strategies. Security is also addressed in this same report.
• **Risks/Liability Associated with multi-source, cooperative applications**	• *Analysis of the liability and risks with DMA application adoption.* • *RESULT:* o *Framework for addressing risks and liability associated with the applications.*	These issues are under review by the ITS Legal Policy team. A white paper on liability and other legal issues is expected in summer of 2012.
• **Intellectual Property**	• *Analysis of the Intellectual property risks associated with each application or application bundle.* • *RESULT:* o *Recommendation for Intellectual property strategies.*	A forthcoming research report titled: ***Policy Analysis and Recommendations for the Open Source Applications Development Portal (OSADP)*** identify intellectual property risks and offer recommendations.
• **Commercialization/Market Adoption**	• *Analysis of the challenges associated with adopting the DMA applications.* • *RESULT:* o *Framework for determining effective paths for market adoption.*	These issues will be informed by a market research effort that will examine the value of data. Other research includes efforts by the ITS Technical Policy team to explore the value associated with having the applications be part of the connected vehicle Core System.

Table ES 4: Research Recommendations for Core System Integration

(A) Critical Policies Issues	(B) Expected Outcomes from Policy Research	(C) Policy Reports
• **Core System Integration**	• *Identification of the value of Core Systems in context of their relationship to the dynamic mobility applications and data environments.* • *Identification of risks resulting in an identification of the role of certification and standards policies.* • *RESULT:* o *Framework for developing policies that govern the DCM and DMA systems, technologies, and applications in their relationship to the Core System.*	These issues will be informed by research includes efforts by the ITS Technical Policy team to explore the value of applications are part of the connected vehicle Core System.

Introduction

The Federal Highway Administration (FHWA), in partnerships with the Intelligent Transportation Systems (ITS) Joint Program Office (JPO), the Federal Transit Administration (FTA), the National Highway Traffic Safety Administration (NHTSA), and the Federal Motor Carrier Safety Administration (FMCSA) are working to research, develop, and facilitate adoption of the next generation of advanced transportation technologies and systems related to mobility and operations. The focus of the current research is on the transformative nature of wireless technologies that create connectivity between vehicles, between vehicles and roadway infrastructure, and with mobile devices—known as the connected vehicle environment. If the connected vehicle technologies prove to be truly transformative, they will significantly reduce safety problems, enhance mobility, and reduce the environmental impact of surface transportation systems.

From the perspective of enhancing mobility, the connected vehicle technologies are expected to generate a higher volume and better quality of data through new sources of vehicle-based data. Using these new data sources to populate open data environments, public sector agencies, private sector firms, and consumers will have access to multi-source, real-time data for synthesis into dynamic mobility applications.

Purpose of this White Paper

This white paper describes the critical policy and institutional issues associated with applying open data and open source policies to connected vehicle systems, technologies, and applications for mobility, specifically during:

- Development, testing, and demonstration phases of new, connected vehicle data capture and management (DCM) technologies, datasets, and systems
- Development, testing, and operations of a new open source applications development portal (OSADP)
- Development and commercialization of new dynamic mobility applications (DMAs).

The U.S. Department of Transportation's (US DOT) Data Capture and Management (DCM) and Dynamic Mobility Applications (DMA) programs have envisioned implementing open data and open source policies as a means of:

- Supporting public sector needs with less costly technologies
- Promoting collaboration and innovation
- Encouraging new market opportunities

Four primary elements of the DMA and DCM programs are considered within this white paper:

1. The DCM program's open datasets
2. The DCM program's open data environments – a Prototype Data Environment (PDE), a Research Data Exchange (RDE), and future envisioned operational environments
3. The DMA programs Open Source Applications Development Portal (OSADP)
4. The DMA program's dynamic mobility applications (DMAs).

The USDOT's interest in developing open data and open data environments and public-sector mobility applications in an open source portal is directly aligned with a broader governmental effort— the *Open Government Directive*— that promotes the principles of transparency, participation, and collaboration with citizens to promote greater involvement in government.

Benefits associated with implementing open data and open source policies are well documented from both a public and private sector perspective. Both the DCM and DMA programs have vision papers[1] that describe the expected benefits from adopting these policies.

This white paper complements those vision papers by documenting the anticipated challenges in a manner that allows for timely focus and resolution. Challenges are defined during the research stages of concept development, prototyping, and testing; and during the stages of technology transfer, market adoption, and commercial operations. The challenges (or critical issues) described in this white paper are a result of a preliminary analysis of the emerging DCM and DMA systems, technologies, and applications; a review of the technical, evolutionary path for both programs; and a review of Federal, State and local, academic, and commercial practices (documented in a separate white paper).

In addition to identifying and describing the critical issues that are most likely to occur, this white paper also establishes the parameters and focus of future research that will result in policy recommendations.

The challenges and critical issues described in this white paper are a result of a preliminary analysis of the emerging DCM and DMA systems, technologies, and applications; a review of the technical roadmaps for both programs; and a review of Federal, State and local, academic, and commercial practices (documented in a separate best practices/lessons learned white paper).

Addressing these critical issues during the research stages may impact how the DMA and DCM technologies, systems, and applications evolve. Similarly, technical progress that helps move the technologies, systems, and applications closer to operations will likely give rise to new policy and institutional issues. The process of identifying, analyzing, and recommending policies is iterative and is most effective when iterations include stakeholders.

It is thus expected that this white paper may be revisited and/or expanded in the future. It is offered at this time as a roadmap to addressing policy issues at appropriate times.

[1] Located at: http://www.its.dot.gov/data_capture/datacapture_management_vision1.htm and at: http://www.its.dot.gov/dma/dma_vision2.htm.

This white paper is divided into chapters that explore and describe the critical issues associated with each DCM or DMA technology, system, or set of applications as follows:

- Each chapter begins with a definition and presentation of a chart that lists the critical issues specific to the technology, system, or application on the left side and the stages of research through commercialization on the right side. The result is to provide the reader with an overall summary of the content to be discussed within the chapter.
- A second table follows that identifies when, during the technical stages, the critical issues may have the most impact (and require options and recommendations for resolution). In providing this second table, the technical research team has a roadmap that helps prioritize when policy and institutional issues will need to be addressed.
- The remainder of each chapter offers a definition of each critical issue and lists the questions as a means of guiding the focus of policy research and analysis (whose results will be documented in a series of upcoming reports). The chapters include:
    - Chapter 1: Critical Policy Issues for Implementing Open Data and for Prototype, Research, and Operational Data Environments
    - Chapter 2: Critical Policy Issues with the Development and Operations of an Open Source Portal
    - Chapter 3: Critical Policy Issues with the Development of New Dynamic Mobility Applications
    - Chapter 4: Critical Policy Issues with Core System Integration

This report is one in a series of six policy reports that describe and analyze the policy issues associated with connected vehicle mobility. The series includes:

- Two foundational reports that identify the critical issues and describe the best practices and lessons learned from government, industry, and academia:
    - ***Identification of Critical Policy Issues for the Mobility Program***, FHWA-JPO-12-035
    - ***State-of-the-Practice and Lessons Learned on Implementing Open Data and Open Source Policies*** (this report), FHWA-JPO-12-030

- Four reports that analyze the specific policy issues in context of the goals of the DMA and DCM programs:
    - ***Policy Analysis and Recommendations for the Open Source Applications Development Portal (OSADP)***, FHWA-JPO-12-031
    - ***Policy Analysis and Recommendations for Development of the Dynamic Mobility Applications***, FHWA-JPO-12-033
    - ***Policy Analysis and Recommendations for the DCM Research Data Exchange***, FHWA-JPO-12-036
    - ***Privacy and Security Analysis and Recommendations for the DCM and DMA Programs***, FHWA-JPO-12-032.

Chapter 1 Open Data and Open Data Environments

1.1 Critical Issues for Open Data and Open Data Environments

To achieve the technical program objectives and offer data in an open data environment, critical policy and institutional issues will need to be addressed through research, analysis, and recommendation of options. The chart below and Table 1 on the next page list the critical issues and identify the technical program stages at which various policy issues will need to be considered:

Critical Policy and Institutional Issues	Technical Research Program Phases
• **Governance/ Data Governance Policies:** o Governance: structure and authority o RDE Data Manager roles and responsibilities o Policies for connecting with external data environments ("federation") o Policies for Maintenance • **Data Environment Policies/ System Rules of Operation:** o Policy on Use of Innovative, Leading-Edge Technologies and Configuration Management o User Access Control Policies/User Registration Processes o Security Policies o Metadata Classification o Quality Assurance o Rules of Conduct / Enforcement and Monitoring o Language Policy o Policy on Use/Application of Standards • **Liability/Risk Mitigation Strategies** • **Intellectual Property Policies** • **Privacy/Data Usage Policies:** o Application of Fair Information Practice Principles (FIPPs) o Privacy and connections with external environments o Data access, storage, and archiving policies • **Business models/Data Ownership Policies** o Public/Private roles with respect to data provision, data use, data access, and data integration • **Application of other Federal Policies** (particularly for hosting data)	• **Acquisition of Test Data Sets** • **Data environments:** o Prototyping a Data Environment (PDE) o Designing, Building, and Operating a Research Data Environment (RDE) o Demonstrating streaming of real-time data and dynamic data integration o Designing, Building, and Demonstrating an operational data environment in support of Dynamic Mobility Applications • **Lessons Learned and Transfer of the Operational Data Environment Specifications and Market Adoption (growth opportunities to improve and expand)**

TABLE 1: POLICY ISSUES BY DCM TECHNICAL PROGRAM PHASE

<table>
<tr><th>Policy Options Needed for:
Program Phase:</th><th>Acquisition of Test Data Sets</th><th>Development of the Prototype / Research Data Environments (PDE and RDE)</th><th>Operations / Management of the RDE</th><th>Demonstrating streaming of real-time data and dynamic data integration</th><th>Demonstrating an operational data environment in support of Dynamic Mobility Applications</th><th>Market Transfer and Adoption</th></tr>
<tr><td>• Governance and Data Governance Policies:
o Governance: structure and authority
o Role of the RDE Data Manager
o Connecting with external data environments (“federation”)
o Policies on Maintenance</td><td>X
(data governance needs defined)</td><td>X
(governance needs defined, informed by ConOps)</td><td>X
(governance policies tested)</td><td>X
(Federation policies tested)</td><td>X
(governance and federation policies in use)</td><td rowspan="4">X
(analysis of market interest based on existing policies – informs business model development)</td></tr>
<tr><td>• Data Environment Policies/System Rules of Operation:
o Policies on Use of Innovative, Leading-Edge Technologies
o User Access Control Policies/User Registration Processes
o Security Policies and Data Access, Storage, and Archiving Policies
o Metadata Classification
o Quality Assurance
o Rules of Conduct / Enforcement and Monitoring
o Language Policy
o Policy on Use/Application of Standards</td><td>--</td><td>X
(policies/rules defined, informed by ConOps)</td><td>X
(policies/rules tested)</td><td>X
(policies/rules tested – inform operational data environment development)</td><td>X
(policies/rules in use)</td></tr>
<tr><td>• Liability /Risk Mitigation Strategies
• Intellectual Property Policies
• Privacy Policy</td><td colspan="2">X
(identification of risks, definition of policies)</td><td colspan="2">X
(testing policies)</td><td>X
(policies in use)</td></tr>
<tr><td>• Business Models/Data Ownership Policies</td><td>--</td><td>--</td><td>--</td><td colspan="2">X
(review of benefits and development of a business model)</td><td>X
(analysis of value)</td></tr>
<tr><td>• Application of other Federal Policies (particularly for hosting data)</td><td colspan="2">X
(i.d. requirement)</td><td colspan="3">X
(policies in use)</td><td></td></tr>
</table>

1.2 Scope of Critical Issues

An appropriate scope for each of the policy issues, and one that is aligned with the technical objectives, is provided as the basis for policy research and analysis:

1.2.1. Governance and Data Governance Policies: A governance structure frames roles and responsibilities in relation to authority (i.e., scope, sanctions, and enforcement). The structure is a stakeholder consensus-based definition for who can take what actions with what information, under what circumstances, and using what methods.[2] It thus establishes the means by which those "governed" are able to influence the overall scope and decisions of the governing body, as well as mechanisms for appeal and/or adjudication of contestable actions. Data governance further extends the definition of governance policies to include the policies on processes that address quality, access, standards, metadata organization, and other issues associated with data.[3]

Questions that form the focus for the policy research in support of open data and open data environments are:

- **Structure and Authority:** What form of governance structure(s) supports open data environments? Who will have what roles and responsibilities in decision making and dispute resolution? Decisions for upgrading and maintaining the data environments? Enforcement? What are the options regarding the level of ongoing federal involvement and, for each option, what are the roles and responsibilities of federal participants and what are the associated costs? Can governance be implemented by the private sector or a hybrid of public- and private-sector stakeholders? Who currently has authority or is new authority needed?
- **Research Data Exchange (RDE) Data Manager:** What is the role of the RDE Data Manager, and are the appropriate policies defined to guide the Data Manager in operations, maintenance, and enforcement?
- **Federation of data environments:** What criteria should determine the appropriateness and eligibility of connecting external data environments with either the research or operational data environments? What are the associated costs and responsibilities of establishing and maintaining a relationship – for both the RDE and the external environments? What policies/rules are needed for adding or removing these external environments? For removing data sets? How does federation support data ownership? Revenue generation from the data ownership? How does federation impact liability or raise security risks? What are mitigation strategies?

[2] Data Governance Framework. Data Governance Institute. At: http://www.datagovernance.com/dgi_framework.pdf.
[3] Sarsfield, Steve (2009). "The Data Governance Imperative," IT Governance.

- **Data Sharing Agreements:** What are standard components of data sharing agreement documents? What are important considerations and lessons learned from other agencies in implementing data sharing agreements?
- **Policy for Maintenance:** Who makes decisions about technology upgrades and flexibility of adding new technologies? Who manages the DCM system configuration?

Expected Outcome from Policy Research:

- *Identification of needs for governance and authority.*
- *Analysis of whether new authorities are needed.*
- *Definition of roles and responsibilities.*
- *Identification of options for policies on federation, data sharing, and maintenance of data environments.*
- ***RESULT:***
  - *Recommended governance policies for Data Environment/Exchanges and for data governance.*
  - *Recommended next steps in developing protocols and procedures.*

1.2.2. Data Environment Policies/System Rules of Operation:

The federated data exchange is likely to result in an interconnected 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 policies/rules of use and operation to ensure that all participants are aware of and follow common practices that ensure interoperability, effectiveness, and protection. Questions that will scope the policy research include:

- **Policy on Use of Innovative, Leading-Edge Technologies and Concepts:** In developing the data environment, there are a host of innovative technologies that can be considered – dynamic interrogative data capture, virtual warehousing, cloud computing, crowd sourcing are among the innovations that will be considered within the scope of the technical research. From a policy perspective, what unique challenges are encountered with these new technologies? If a concept such as cloud computing were used, what are the policy and institutional implications of putting responsibility of a key element (such as data servers) into a third party's hands? How do such risks compare to the traditional options of capital investment? Are the innovative technologies for enabling data environments capable of being market-ready when the applications are market-ready?
- **Policy on User Access Controls/User Registration Processes:**
  - At what points will user access be controlled? What are options for controls and which options are relevant to the RDE?

- With registration, what (if any) descriptive data is to be obtained from users, and why?
- Given the multiplicity of users, is there a need to gather information on which data the user wants to access and what the user plans to do with it? What purpose would such information serve? Will collection of such information assist with the evolution of the data sets and data environments to be more relevant and user-friendly? What are the privacy and industry concerns?

o **Security:** Security forms the basis for trust, a critical element in market and user adoption. Yet higher levels of security to ensure data protection are often in conflict with the concept of open data and open data environments. Questions are:

- What is the appropriate level of security needed to create user trust? How will it impact the concept of open data? Are any data considered "mission-critical"? Will these data require more security than other data?
- Is it possible to apply different levels of security within the data environments?
- What are policies on data access, storage, and archiving? How do they support the privacy policies?

o **Metadata:** Metadata is documentation that defines and describes the data. This documentation is a means of organizing the data so that the user can easily find and access the relevant data. Questions include who will develop and maintain the metadata framework for the new data environments? How will changes be incorporated over time? Who has the right/role to request changes?

o **Data Quality Assurance:** Data quality assurance is the process of profiling data to discover inconsistencies and other anomalies, and performing data cleansing activities (e.g. removing outliers, missing data interpolation) to improve data quality. These activities can be undertaken as part of Data warehousing or as part of the Database administration of an existing piece of applications software. For connected vehicle data to be relevant, it must be of high quality if it is to support mobility applications and, further, accurate if the data is to be used in safety. DMA application developers and other developers and system users must have confidence that the data exchange has in place policies and procedures to ensure data quality.

From a policy perspective, an acceptable baseline for quality will need to be developed and data quality standards developed. Additionally, policy development will need to address the choice of which tools to employ to identify and mitigate errors as a means of mitigating liability risks. There are various options for checking and assuring the quality of the data. In particular, the Center for AIDS Research Network of Integrated Clinical Systems, and the National Data Buoy Center stand out as having rigorous quality processes in place that make creative use of automated techniques for real time data quality verification. It is likely that the DCM / DMA programs will need to go well beyond even this level of data quality assurance, and include formalized

protocols for data review, error documentation, and error correction. Notably, all of the options have cost implications. Policy research needs to review the options and trade-offs and identify which options are best suited for data environments that host real-time data and data exchange. Questions include:

- What is the baseline that defines the level of quality necessary for the connected vehicle data, data environments, and mobility applications?
- Will the data environments be required to apply tools for data quality checking? If so, what are the costs and who will be responsible? What performance metrics will the tools need to meet? How will these tools affect/impact the real-time aspect?

- **Rules of Conduct / Enforcement and Monitoring:**
  - What defines user misbehavior in the Data Exchange , and how should this be monitored?
  - What sanctions is the DCM program prepared to impose on bad actors? Would it be prepared to prosecute under any circumstances?
- **Language Policy:** Will there be an established common language? If multiple languages are employed, what impact would it create in the administration of the program in terms of: number of websites, reference guides, and/or translators? Who will provide the funding?

- **Standards:** Standards are a critical element in interoperability. Questions that will scope the policy research include:
  - Are there data format standards that are needed? Other standards? Data quality standards?
  - What is the policy for use of standards within the data environments? For the data? For the metadata?

Expected Outcome from Policy Research:

- *Analysis of risk and identifications of policy options that address technologies and design, user access and control policies, security, metadata, data quality assurance, rules of conduct, enforcement and monitoring, language policy, and application of standards.*
- ***RESULT:***
  - *Policy recommendations and framework for developing system rules of operation.*

1.2.3. Liability/Risk Mitigation Strategies:

A wide range of data environments exist in practice today. Typically, these data environments have clear data and system ownership and are guided by the ownership's policies regarding liability and privacy. Risks are determined by the type of data housed in the environments and the data's purposes, uses, and level of criticality. While these data environments can be reviewed for best practices, the connected vehicle data environments

introduce a new element of risk – multi-sourced data is fused to provide a "cooperative " understanding of the impending risks and conditions within the connected vehicle environment. Questions that will address the scope of the policy research regarding liability have to do with both ownership and privacy and include:

- What are the liability risks associated with the connected vehicle data environments? Can they be constructed in a manner that limits or reduces these risks?
- Who is liable when data sets are combined or fused from multiple sources?
- If a data set containing PII is erroneously placed within the data environment and if a user with approved access misuses the PII, what is the risk that DOT might be held liable for any injuries or costs to the PII owner? How can that risk be mitigated?

Expected Outcome from Policy Research:

- *Identification of liability risks and identification of new liabilities introduced by connected vehicle data capture and management and open data.*
- ***RESULTS:***
  - *Risk Mitigation policy recommendations.*

1.2.4. Intellectual Property Policies: In identifying intellectual property issues in relation to the data environments, the following questions must be resolved by experts regarding use of intellectual property under open access conditions:

- What licenses exist to support open data and public accessibility (or broader accessibility)? How might the license terms support or impede the DCM program's objectives? Are these licenses in conformance with the Federal Acquisition Regulation and any other relevant US regulations?
- Does the DCM program need to receive an additional license each time the same individual or entity contributes a new or enhanced data set to the RDE? How does licensing differ with the in an operational setting?
- Who owns the intellectual property if the connected vehicle data sets are combined/fused from multiple sources?
- Who owns the intellectual property if a contributed data set is a corrected version of the original data set, but corrected by other entities than the original owner: the owners of the original, or the contributor?
- If a contributor is located outside of the US but wants to contribute an enhanced set of US transportation data, are the contributor's IP interests protected by the laws of the host country or the laws of the US?
- Does streaming data differ from other forms of intellectual property? How can intellectual property be captured with streaming data? What are the existing models?

Expected Outcome from Policy Research:

- *Analysis on intellectual property risks associated with an open data environments (RDE) and the datasets.*
- ***RESULT:***
  - *Policy recommendations to protect intellectual property.*

1.2.5. Privacy/Data Usage Policies: Comprehensive Federal privacy policies go beyond the mandate regarding collection of Personally-Identifiable Information (PII) to include best practices in transparency surrounding the intent of data collection, use, and analysis. These best practices are known as Fair Information Practice Principles (FIPPs) and they establish a clear basis for identifying what data is needed and what data does not need to be collected. FIPPs are based on the notion that those who are generating data are clear on the purposes for the data and that the generators have the ability to choose to provide the data (known as "opt-in" practices). With regard to open data and open data environments, the questions that focus the policy research are:

- **Application of FIPPs:** FIPPs are a Federally-recognized best practice for data management – will they be applied for the data environments and how will they set policies for the data access/use/archiving for the data environments? Will they need to vary in relation to the type of data that is collected and openly available? Are there tools for mitigation such as filters or software that anonymizes or scrubs data? Will they be used with the open data environments? What are the costs or other technical implications for requiring use?
- **Connections with External Environments:** What is the policy for managing privacy concerns when external data environments are connected and may contain or be collecting data with PII? What privacy safeguards are needed for the data environments in terms of user access to data, as well as monitoring and enforcement procedures, to ensure the highest level of adherence to the FIPPs?
- **Multi-Source, Synthesized Data:** What are the privacy implications if contributed data sets that combine and integrate multiple original data sets contain privacy data, and are posted in the federally managed data environment?

Expected Outcome from Policy Research:

- *Privacy analysis for the datasets and the RDE regarding use of PII.*
- ***RESULT:***
  - *Initial application of the Fair Information Principle Practices (FIPPs).*

1.2.6. Business Models/Data Ownership Policies: A critical set of questions concerns data ownership. Who owns what data and, based on ownership, what are the options for using the data? In an open data environment, how does ownership impact the ability to capture value? Does capture and management of the data result in services that need to be paid for? By whom? Can the services to capture and manage the data be financially supported by the value of the data? If so, does this result in a less open or closed data policy? How might this be viewed from the perspective of monopolistic practices?

Importantly, if the connected vehicle data has value and that value is assessed at levels that are of interest to private sector firms, new business models and/or partnerships may evolve to provide the networks, security, and Core System capabilities. Because despite solid policies and proven technologies, if a business model for financially sustaining the operations and maintenance of the data environments is not feasible, the data environments and dynamic data exchange will not be adopted by agencies or the market. With implementation of the RDE, a longer term analysis of lessons learned will include:

- Identification of the cost elements, revenue opportunities, and other economic impacts associated with installing, operating, and maintaining the data environments and supporting dynamic, real-time data fusion and exchange.
- Identification of guidance, training, and/or tools needed to support the workforce.
- Analysis of the value proposition that would attract investors or partners along with identification of potential sources of funding; institutional options for owning and/or operating data environments; and identification of growth or expansion opportunities.

Further, in conducting a legal analysis of the options for data ownership policies, the impact to the future market will need to be explored.

Expected Outcome from Policy Research:

- *Analysis and options for data ownership.*
- *Market research to identify the potential value of the new, vehicle-based data and comparison against the costs of capturing and managing it in a secure environment.*
- *Market adoption/commercialization of the data environments.*
- ***RESULT:***
  - *Options for new business models/partnerships based on analysis of the RDE implementation lessons and cost elements and revenue options for financially sustaining data environments.*

1.2.7. Application of other Federal Policies: The initial data environments will be directly funded from Federal funds and operated using Federal and federally-contracted staff, and by applying existing Federal policies.. Questions that will scope the policy research include:

- Which other Federal policies apply to the DCM program?
- Under what conditions do DCM data have to / should be made 508 compliant?
- How does providing DOT data relate to the Open Data.gov initiative?

Expected Outcome from Policy Research:

- *Identification of other Federal policies that may be required for the datasets, the RDE, or operational environments.*
- ***RESULT:***
  - *Recommendation on what Federal policies apply and analysis of the impact.*

As part of future research, other federal policies will be reviewed and analyzed for their relevance, specifically:

- **The Americans with Disabilities Act (ADA) and the 508 Compliance Requirement**
- **March 2011 DOT Data Release Policy, Order 1351.34**
- **The Department of Energy's Secure Transportation Data Project**

Chapter 2 Open Source Applications Development Portal (OSADP)

2.1 Critical Issues for OSADP

The OSADP is a virtual application development environment and is intended to support the research, analysis, application development, and testing of dynamic mobility applications. By investing in open source research, the DMA program expects to address high costs, risks, and concerns of stakeholders that result from uncoordinated, proprietary and duplicative applications research and testing; higher costs for the commercialization and integration of non-interoperable or proprietary technologies and control systems; and slowed progress towards a less desirable and ad-hoc sub-optimal end-state.[4]

The OSADP will have the following major characteristics:

- A **web-based portal as the primary access** for all Internet users.
- An **application development environment** that enables software developers and registered users to participate in building mobility applications.
- An **open source community environment** with collaboration tools that enable communication among the registered users. This community is protected and user registration is required to access it.
- A **released open source repository** which hosts application files including source code and associated documents and artifacts.
- **Governance and license terms** for all portal users.

The critical policy issues and technical research phases are listed in the chart on the next page:

[4] Source for rationale and basis for the Open Source Program comes from the white paper, *Dynamic Mobility Applications Program Vision: Objectives, Core Concepts and Projected Outcomes*, April 2010 at: www.its.dot.gov/dma/dma_vision2.htm.

Critical Policy and Institutional Issues	Technical Research Program Phases
• **Program and Portal Governance Policies (addresses system governance for the web-based portal and the community environments; also system decision making and conflict resolution). Policies include:** o Governance Models/Roles and Responsibilities o Federal Role in OSADP Governance o Business Model o User Access and Controls o Rules of Conduct o Language Policy o Security • **Project Governance Policies (addresses user controls and access policies for the Applications Development Environment and Applications Release Repository [herein referred to as the "repository"]; also rules of conduct). Policies include:** o Management Approach to Projects o Policies for Collaboration and User Access which further includes: ▪ *Permissions/Openness* ▪ *User Classes* ▪ *Rules of Conduct* ▪ *Bundle versus Application Access Controls* ▪ *Project Forking Policy*[5] ▪ *Repository Access* ▪ *Contributor Recognition* ▪ *Use of Standards* • **Intellectual Property and Copyright/Licensing and Liability** • **DMA Development and Procurement:** o Choice of Development and Procurement Strategies o Federal Staff, Resources, and Costs o Applications Suitability for Portal Development o Criteria for Acceptance of New Applications Development o Criteria for Release into the Repository • **Product Liability Issues** • **OSADP Business Model**	• **Concept of Operations (Phase 1 – Summer 2011)** • **Development and Testing of the Open Source Portal (Phase 1 – Summer 2011-Spring 2012)** • **Deployment of the Open Source Portal (Phase 2 – Summer 2012-2013)** • **Operations and Management of the Open Source Portal (Phase 3 – 2013-2015)**

Table 2 on the following page aligns the policy issues against the different stages of the OSADP development effort and identifies the stages when policy analysis and options are needed most.

[5] Creation of a new branch of an application or database that is independent of the original.

TABLE 2: POLICY ISSUES BY OSADP TECHNICAL PROGRAM PHASE

Policy Options Needed for: / Program Phase:	Concept of Operations (Phase 1 – Summer 2011)	Development and Testing of the Open Source Portal (Phase 1 – Summer 2011-Spring 2012)	Deployment of the Open Source Portal (Phase 2 – Summer 2012-2013)	Operations and Management of the Open Source Portal (Phase 3 – 2013-2015)
• **Program and Portal Governance Policies**	**X** (needs/policy options defined – informed by OSADP ConOps & SyRS)	**X** (policies prototyped and tested)	**X** (policies in use)	
• **Project Governance Policies**		**X** (needs/policy options defined – informed by DMA ConOps & SySR)	**X** (policies developed, prototyped and tested)	**X** (policies in use)
• **Intellectual Property and Copyright/Licensing and Liability**		**X** (needs/policy options defined – informed by DMA ConOps)	**X** (legal review and policies developed, prototyped and tested)	**X** (policies in use)
• **Product Liability Issues**	**X** (risks identified)	**X** (legal review and mitigation strategies identified)	**X** (mitigation strategies implemented)	
• **DMA Development and Procurement Strategies**	**X** (policy options identified)	**X** (legal and procurement review and strategies identified)	**X** (policies in use)	
• **OSADP Business Model**			**X** (identification of value/alternative ownership options)	

2.2 Scope of Critical Issues

An appropriate scope for each of the policy issues, and one that is aligned with the technical objectives, is provided as the basis for policy research and analysis:

2.2.1. Program and Portal Governance Policies: The OSADP governance will require policies at two levels—at the programmatic and portal levels (systems level) and at the project level. At the system level, policy research will include:

2.2.1.1. Governance Models/Roles and Responsibilities: What are other portal governance models and what are the pros/cons and trade-offs among them? Who will make decisions and what are the processes needed in support of an operational portal (i.e., registration, revocation of rights, enforcement, among others)?

2.2.1.2. Federal Role in OSADP Governance: What are the options regarding the level of ongoing federal involvement needed? For each option, what are the roles and responsibilities of federal participants, and what are the associated costs? What are the federal policies, regulations, and guidelines regarding restrictions on the foreign export of federally-funded research materials? How will these policies be enforced? What level of resource support should be included in the Service Level Agreement?

2.2.1.3. Business Model: Who will fund the development, operations, and maintenance of the portal? Is there a market-basis that will allow the Federal government to shift the portal to the user community?

2.2.1.4. User Access and Controls: Will the portal's development environment be open and accessible to all? What terms and conditions should control or potentially restrict user access?

2.2.1.5. Rules of Conduct: How will monitoring for misbehavior or misuse of the Open Source Portal be conducted? What should be the basis for sanctions if misbehavior or misuse is detected? What sanctions would be appropriate and enforceable?

2.2.1.6. Language Policy: Will there be an established common language? If more than one language is employed, will there be multiple websites, reference guides, and/or translators? Who will provide the funding to support any additional languages?

2.2.1.7. Security: What are the potential security risks for the OSADP? What are options for security that balance the desire for transparency with the need to secure against misbehavior?

Expected Outcome from Policy Research:

- *Identification of options for OSADP program and portal-level governance.*
- *Analysis of model effectiveness for achieving the DMA program goals for rapid, collaborative application development with transparency and the ability to retain rights for software licensing/ distribution to public agencies.*
- ***RESULT:***
  - *Recommended steps for implementation.*

2.2.2. Project Governance Policies: The applications that will be developed within the OSADP are likely to be highly diverse, including spanning ranges from highly collaborative (and thus requiring open access policies) to those applications with sensitive data or proprietary source code (and thus requiring less-open and more secure policies). The following elements define project level governance policies:

2.2.2.1. Management Approach to Projects: Portal management approaches can range from directed approaches to guided approaches to meritocratic approaches. As a policy, these approaches describe the types of project leadership and staff roles that are expected within the portal. Can the OSADP support different types of management approaches, including hybrids, based on project needs? What approaches best support DMA development?

2.2.2.2. Collaboration and User Access: Questions that scope the policy research include:

- **Permissions/Openness:** Should all application development projects be open to all Portal registrants? What factors should influence these decisions? What are the policy options? If not, where should user access controls be imposed in relation to application development? If permission requirements are put in place, what information should accompany a request for access? Is this information for descriptive purposes only, or for assessment of the user? If the latter, what criteria are relevant? How and by whom should the review of this information and decision regarding access permission be conducted? How will requests from foreign developers be treated? If not from the U.S., will there be a higher level of information required before access is permitted?
- **User Classes:** Are there different classes of users? Who determines the classes? How are user classes defined? Who might be excluded and how does exclusion protect against risks such as security or access to proprietary information, among others? Is there a redress process if excluded?
- **Rules of Conduct:** What rules of conduct should be established for users of the Application Development Environment? What should be included in the Project Participation Agreement?
- **Bundle versus Application Access Controls:** When the DMA program announced its selection of high-priority applications for development in January 2011, the applications were grouped into bundles on the basis or shared data needs or the need for coordinated development across the applications. However, policy research since then has shown that coordination across bundles is also needed. What policies are needed to structure user access controls to enable OSADP managers to assign the appropriate authorizations to users that permit cross-communication and collaboration? Should the OSADP strictly control user access to the development projects for those applications in the interest of public safety? Alternatively, can the program take the position that deployer firewalls will be relied on to ensure public safety, and leave access to the development project open?
- **Project Forking Policy:** Open source development offers the possibility of forking or, creating a new branch of an application or database that is

independent of the original. How should the OSADP accommodate project forking? What are the risks and the benefits? Are there particular points at which forking should be allowed, for instance after release into the Repository? How should policies for forking be developed—based on risk, based on agreement by a sufficient number of community members, or both?

- **Repository Access Policy:** Are user access controls needed for the Repository? Should all completed applications be made available to all through the OSADP's Repository? What rules of conduct should be established for users of the Repository? Should they be different in any way from those for the Application Development Environment?
- **Contributor Recognition Policy:** A governance structure will clearly identify the rights, responsibilities, and opportunities for Users and Contributors of applications and their associated source code, algorithms, programming and enhancements, and data. What are appropriate policies for the OSADP to provide recognition for individual or team contributions to the portal and/or to the applications? Is there a way to program this recognition or must it be done through manual processes?
- **Use of Standards:** Will policy require the use of particular standards in the development of the OSADP? Are there typical industry standards for portals?

Expected Outcome from Policy Research:

- *Identification and analysis of options and policy recommendations for OSADP project-level governance (includes recommendations for management approach to projects, policy on collaboration and user access which further includes permissions/openness, user classes, rules of conduct, bundle versus application access policies, Project Forking policy, repository access policy, contributor recognition policy, and policy on use of standards).*
- ***RESULT:***
  - *Recommended steps for implementation.*

2.2.3. Intellectual Property and Copyright/Licensing: The open source licensing policies for the OSADP protects IP rights of Contributors without hindering continued innovation and commercialization. Questions to focus policy research are:

- How does the choice of open source license terms affect use of the OSADP for applications development?
- What must the OSADP do in support of license arrangements to track the intellectual property associated with applications development and enhancements to released applications?
- Should the program determine which open source license(s) is/are acceptable, or should the choice of license or other formal arrangement properly be the decision of the software developer?

- Which open source licenses are preferable for use? What are the different characteristics of these licenses, and do any have distinct advantages or disadvantages? Are there specific license terms that would make some license categories unacceptable relative to the DMA program's goals and objectives?
- If more than one license form is used for any reason, what are the operational implications?
- How are applications developed within USDOT protected by copyrights and other legal terms and conditions? How do these terms and conditions align with the licensing arrangements?
- Are there patents in force that would interfere with development of any the applications identified for development by the DMA program? How can such be identified in advance to mitigate against latent infringement claims that would adversely impact applications once developed and deployed?
- How can licensing be structured such that the Federally-funded applications can be licensed for free or a nominal fee to public sector agencies? What impact might this have on existing markets?
- What IP provisions are needed relative to permitted Project Forking initiatives?

Expected Outcome from Policy Research:

- *Analysis on intellectual property associated with the dynamic mobility applications.*
- ***RESULT:***
  - *Policy options and recommendations.*

2.2.4. Product Liability: What liability and security risks are associated with the new applications? How do those risks differ from existing applications? Will the licensing / indemnification arrangements address issues associated with liability of applications once these leave the OSADP and is that an adequate mitigation strategy?

Expected Outcome from Policy Research:

- *Identification of risks and analysis on whether the new, dynamic mobility applications, in particular, those offered as free and open source software, introduces any new liabilities.*
- ***RESULT:***
  - *Recommended risk mitigation options.*

2.2.5. DMA Procurement Strategies: Applications development may be procured through a host of strategies ranging from traditional government procurement method (i.e., Request for Proposals) which have clearly delineated defined roles and responsibilities of the applications development and Federal staff to more undefined options such as challenge grants/prizes or Federally-managed agile development contracts in which the roles and responsibilities are less defined and more likely to include iterative processes and flexible definitions of who may participate. To support different types of applications development based upon the procurement strategy used, the OSADP will need to consider policies and options for:

2.2.5.1. Procurement Strategy: Are the OSADP policies and structures supportive of the DMA procurement strategies?

2.2.5.2. Federal Staff, Resources, and Costs: Are there differences in the demand for federal participation during development, depending on the software development methodology the developer employs? If so, what are the associated costs and benefits to the program? Does the program have access to federal personnel with the required skills?

2.2.5.3. Applications Suitability for Portal Development: Are all applications suitable for development on the OSADP?

Expected Outcome from Policy Research:

- *Identification of risks and opportunities associated with the development and procurement of the applications. Identification of implications for the OSADP.*
- ***RESULT:***
  - *Recommended procurement and development strategies for achieving the DMA program goals for rapid, collaborative development and ability to retain rights with least amount of risk regarding intellectual property infringement or exposure of sensitive source code or data.*

2.2.6. OSADP Business Models: In an ideal conclusion to the research program, the connected vehicle technologies, systems, and applications will eventually be transferred to academic and private sector ownership and operations. The OSADP presents a complex case as the system is funded for a very specific research purpose – to develop the dynamic mobility applications. Recent considerations, however, suggest a scenario under which the DMA development has ended or Federal program managers decide to no longer sustain the OSADP. At this point, is there a viable partnership or business model that would allow for the transfer of ownership for some or all of the OSADP? Does the OSADP configuration and policies present an obstacle to valuing this particular open source portal? To whom would the OSADP have value? Would changes be needed to make it a viable commercial system? Who will pay for the changes?

Expected Outcome from Policy Research:

- *Exploration of an OSADP business model for private sector or academic ownership and operations.*
- ***RESULT:***
  - *Framework for determining whether the OSADP might have value post-research.*

As part of future research, other federal policies will be reviewed and analyzed for potential relevance, specifically:

- **The Department of Defense's *2011 OTD Lessons Learned: Open Technology Development (OTD) Lessons Learned & Best Practices for Military Software***
- **The Department of Transportation's TRANSIMS Portal.**

Chapter 3 Development, Market Adoption, and Operations of Dynamic Mobility Applications

3.1 Critical Issues in Developing and Implementing Dynamic Mobility Applications

The DMA program positions the federal government as a technology steward for the continued evolution of integrated transportation system. Two core concepts, in particular, guide the vision, namely:

- ***Leverage Multi-Source Data:*** The new dynamic mobility applications will fully leverage high-quality, integrated, multi-source data. These applications may target specific modes (e.g., supporting freight vehicles automated safety checks) or may be multi-modal in nature (e.g., a traveler information service integrating tolling, transit and parking costs for pre-trip planning). A subset of multi-modal applications, termed cross-modal applications, refers specifically to system management functions that coordinate control between modes and jurisdictions. Of particular importance in leveraging multi-source data is an assessment of the most appropriate methods of capturing and synthesizing the data necessary for supporting a proposed portfolio of mode-specific and multi-modal mobility applications.
- ***Develop and Test Mode-Specific and Multi-Modal Applications:*** In addition to leveraging multi-source data, the applications themselves are coordinated to serve multiple end users. This includes tailoring (with as little duplication of effort as possible) foundational elements like travel time calculation for different users, e.g., system managers, transit or freight fleet operators, or travelers moving among modes. Applications development and testing will include assessment of multiple competing wireless communications platforms for achieving new forms of connectivity among vehicles, roadside infrastructure, and mobile devices.

To achieve the technical objectives of expediting development, testing, commercialization, and deployment of innovative mobility applications, the following chart lists the policy and institutional issues that form the policy requirements; Table 3 on the following pages aligns them with the stages of the program:

Critical Policy and Institutional Issues	Technical Research Program Phases
• Development and Procurement Strategies • Data Privacy • Risks/Liability Associated with multi-source cooperative applications • Intellectual Property • Commercialization/Market Adoption	• Concept of Operations (Phase 1: Spring 2011-Spring 2012) • Investment Decision and Development of Applications (Phase 2: Summer 2012-Winter 2013) • Testing of the Applications in Regional Pilot Test Beds (Phase 3: 2014-2015) • Market Adoption of Applications (Phase 3: 2015-Future)

TABLE 3: POLICY ISSUES BY DMA TECHNICAL PROGRAM PHASE

Policy Options Needed for: / Program Phase:	Concept of Operations (Phase 1 – Spring 2011-Spring 2012)	Investment Decision and Development of Applications (Phase 2 – Summer 2012-Winter 2013)	Testing of the Applications in Regional Pilot Test Beds (Phase 3 – 2014-2015)	Market Adoption of Applications (Phase 3 – 2015-Future)
• **Development and Procurement Strategies**	**X** (needs, policy options defined)	**X** (policies prototyped and tested)	**X** (policies in use)	
• **Data Privacy**		**X** (needs, policy options defined – informed by DMA ConOps)	**X** (policies prototyped and tested)	
• **Risks/Liability Associated with multi-source cooperative applications**		**X** (needs, policy options defined – informed by DMA ConOps)	**X** (policies prototyped and tested)	**X** (policies in use)
• **Intellectual Property**	**X** (needs, policy options defined – informed by DMA ConOps)	**X** (licensing recommendations provided)	**X** (policies in use)	
• **Commercialization/Market Adoption**	**X** (policy options identified)		**X** (policies in use)	

3.2 Scope of Critical Issues

An appropriate scope for each of the policy issues, and one that is aligned with the technical objectives, is provided as the basis for policy research and analysis:

3.2.1. Development and Procurement Strategies: The DMA program is considering use of a combination of conventional procurement and challenge grants to fund application development, depending upon the application. Policy research questions on strategies include:

- Which development strategies most effectively support the development of the mobility applications? What criteria are used to decide which strategy to recommend? What implications do the recommendations have for developing the applications in the OSADP, if any?
- What procurement strategies appropriately balance the program's desire for open, collaborative development with the need for a structured deliverable/timeline? What factors affect the choice of strategy?
- How do conventional procurement and challenge grant processes differ in the timing of when the licensing agreement between the developer and the program is sealed? What implications do such differences have for the content of information provided at the outset to potential respondents?
- Will all funded applications be developed using the OSADP? What factors will determine this?
- Different applications will require different data sets with different sensitivities (for instance, the data associated with public safety). Do such sensitivities affect the choice of procurement strategy? What are the potential risks associated with using the wrong strategy? What opportunities might be missed?
- Does the FHWA have the necessary transactional authority to use different or innovative procurement strategies?

Expected Outcome from Policy Research:

- *Analysis of procurement options for each DMA application bundle.*
- ***RESULT:***
  - *Recommendation of appropriate development and procurement strategies for the applications.*
  - *Identification of implications for the OSADP design and operations.*

3.2.2. Data Privacy: Some applications might require or might be significantly more effective if information that could be considered "personally-identifiable" was included as part of the application (for instance, cellular phone applications for

requesting route information require that the information provider know the device identity). While the applications that are Federally-funded (and thus governed by an agreement) are likely to be restricted to ensure no personally-identifiable information, other applications brought to the OSADP (known as Federally-sponsored) may involve personally-identifiable information. Research questions include:

- What privacy requirements should guide the development of DMA applications if Federally-funded? If Federally-sponsored but not funded?
- What contractual wording is needed to stipulate expectations for privacy-related conduct by software developers within the OSADP?
- What rules of conduct are needed to ensure that non-funded application developers fully divulge the potential uses of personal data so that the public can make an informed decision whether to use the application or opt-in to the data gathering and its uses? Are such rules needed?

Expected Outcome from Policy Research:

- *Analysis of privacy requirements associated with each application and application bundle.*
- ***RESULT:***
  - *Initial application of the Fair Information Principle Practices (FIPPs).*

3.2.3. Risks/Liability: With multi-source data supporting applications, the DMA program may be establishing new ground in terms of liability. Research questions include:

3.2.3.1. Liability of multi-source applications: If a deployer adopts an application that captures and integrates data from multiple sources and the application fails with cost impact, who is liable? Would liability rest on the application developer(s) or the Federal program that provided the funding? What about providers of the data? When are they liable, if at all?

3.2.3.2. Additional questions:

- How do open source licenses address the matter of liability? What terms should the program seek?
- If there is an algorithm error that goes unrecognized until after the application enters the production chain and is adopted, and the error results in negative consequences (crashes, congestion, problems with emergency response, etc.), who is liable? What is the probability of occurrence of each of these situations?
- Is there sufficient established case law to address the policy questions?
- To what extent does the existence or lack of case law offer a real and significant impediment to deployment?

Expected Outcome from Policy Research:

- *Analysis of the liability and risks with DMA application adoption.*
- ***RESULT:***
  - *Framework for addressing risks and liability associated with the applications.*

3.2.4. Intellectual Property: The DMA program intends to offer developed applications using open source licensing. The developers of those applications, who own the intellectual property, must first license the program to do so. Policy research questions include:

- What is the relation between the license the developer provides the program, and the license the program offers to deployers and commercializers?
- What license terms support or impede program goals for application deployment and/or commercialization?
- What license terms assure that funded applications can be offered for free or for a nominal fee?

Expected Outcome from Policy Research:

- *Intellectual property strategies associated with each application or application bundle.*
- ***RESULT:***
  - *Recommendation for intellectual property strategies.*

3.2.5. Commercialization/Market Adoption: Typically, adoption of products based on open source software is not free – adoption may require the purchase of additional hardware, personnel to adapt to existing systems, or maintenance support, among other potential costs.[6] Research questions in support of market adoption include:

- For each application or bundle, what are the cost elements associated with public sector agency adoption? What are potential problems with integrating open-source systems with legacy systems that use proprietary software?
- There is a predominant culture of agencies expecting support for a product after installed. How would support be provided with the DMA applications? Are agencies willing to take complete ownership? Do agencies have the workforce capacity to handle this?

[6] http://searchdatacenter.bitpipe.com/detail/RES/1283262087_26.html; accessed 11/1/2010.

- What mechanisms need to be in place to ensure successful technology transfer to the marketplace? Are there other federally fostered software development initiatives that might serve as models?
- Do some States have policies/laws/standards governing procurement and/or adoption of open source software? Encouraging or prohibiting it? What are best practices? In States that prohibit procurement of open source software, but are silent on adoption, what are the issues with agency adoption from a legal perspective? From an institutional perspective (need for support/training)?

Expected Outcome from Policy Research:

- *Analysis of the challenges associated with adopting the DMA applications.*
- ***RESULT:***
  - *Framework for determining effective paths for market adoption.*

The Concept of Operations for each of the application bundles will significantly inform the policy recommendations. Because these technical documents will not be available before summer/fall of 2012, this critical issues chapter will be reviewed and revised at that time.

Chapter 4: Core System Integration

4.1 Critical Issues in Integrating the DCM and DMA Technologies with a Core System

The concept of a Core System provides the foundation for entities that wish to exchange data with one another to have trustworthy credentials. To satisfy the requirements of the Core System, the design of the data environments and the mobility applications may need to incorporate trust credentials.

The Core System provides two important functions for the connected vehicle world: the opportunity to gain access to trust credentials and exchange data in a secure environment; and it plays an important role as a navigator for locating the data needed from the data environments to support the applications. Critical policy and institutional issues associated with integrating the data environments and dynamic mobility applications with the Core System include:

- What constitutes a minimum Core System and how would it provide value to users who are currently using existing communications platforms for their applications?
- What is the capacity of a Core System's bandwidth and what are policies on use and unrestricted use? What are associated costs? What messages will have prioritization? Who will design, implement, and enforce the message prioritization?
- When an application is developed for the connected vehicle Core System, will it require undergoing a certification process? Can an application that is developed for operations on a connected vehicle Core System still use other communications (non-connected vehicle) networks?
- It is envisioned that applications will receive their trust credentials as part of a certification process. How will data environments receive their trust credentials? Who makes the decision about which data environments meet the criteria? Is there a certification process for data environments?
- What is the impact of agencies choosing not to use the connected vehicle Core System for their applications?
- The policies in support of Core Systems may result in an ability to tailor the Core System to local needs. If this flexibility is built in to the Core System design, will the differences in characteristics affect/impact the applications? What type of consistency is needed to ensure that applications work across Core System boundaries?

Other questions and issues are likely to arise as part of a forthcoming research initiative to identify policy and institutional issues with regard to the Core System as a whole. The policy analysis will include a review of the Core System Concept of Operations, System

Requirements, and Architecture documents that are available as of fall of 2011. The policy analysis is expected to be a two-step process—first analyzing the policy issues specific to the Core System and then identifying the impacts when in use with the DCM and DMA systems, technologies, and applications.

Expected Outcome from Policy Research:

- *Identification of the value of Core Systems in context of their relationship to the dynamic mobility applications and data environments.*
- *Identification of risks resulting in an identification of the role of certification and standards policies.*
- ***RESULT:***
    - *Framework for developing policies that govern the DCM and DMA systems, technologies, and applications in their relationship to the Core System.*

Chapter 5: Summary

This white paper examines the major systems, technologies, and applications that are needed to provide connected vehicle mobility—new data environments, new data sets, a new system and tools for applications development, new applications, and the Core System concept. Upon review of these elements, this white paper identifies the critical policy and institutional issues that may present obstacles to development and implementation.

The critical issues are described in context of the technical research roadmaps as a means of identifying when policy recommendations will be needed to support continued technical development and eventual testing, operations, technology transfer/ commercialization, and market adoption. In this respect, this white paper forms a roadmap for conducting the policy research for the connected vehicle mobility programs.

APPENDIX A. List of Acronyms

BTS	Bureau of Transportation Statistics
ConOps	Concept of Operations
DCM	Data Capture and Management
DMA	Dynamic Mobility Applications
DOT	Department of Transportation
DSRC	Dedicated Short-Range Communications
FTA	Federal Transit Administration
FHWA	Federal Highway Administration
IP	Intellectual Property
IT	Information Technology
ITS	Intelligent Transportation Systems
JPO	Joint Program Office
OD	Open Data
OS	Open Source
OSADP	Open Source Applications Development Portal
PDE	Prototype Data Exchange
PII	Personally-Identifiable Information
RDE	Research Data Exchange
V2I	Vehicle to Infrastructure
V2V	Vehicle to Vehicle
VII	Vehicle-Infrastructure Integration

APPENDIX B. List of Sources

To identify the policy issues that directly impact the success of achieving the DCM and DMA programs' vision and technical objectives, the following documents and events provided important inputs:

- **For overall context and Federal goals:**
  - The US DOT's Strategic Plan, 2006-2011: http://www.dot.gov/stratplan2011/
  - The ITS Strategic Research Plan, 2010-2014: http://www.its.dot.gov/strategic_plan2010_2014/index.htm
  - A stakeholder workshop held in Washington DC in December 2010 that helped define and prioritize the dynamic mobility applications
- **For open data and data environments:**
  - The DCM Program objectives, as taken from the ITS Strategic Plan: (http://www.its.dot.gov/data_capture/data_capture.htm)
  - The DCM vision document, ***Real-Time Data Capture and Management Program Vision: Objectives, Core Concepts and Projected Outcomes***, located at: (http://www.its.dot.gov/data_capture/datacapture_management_vision1.htm)
- **For the open source portal and dynamic mobility applications:**
  - ***A Concept of Operations – Dynamic Mobility Applications Open Source Application Development Portal*** (August 2011)
  - A System Requirements document titled, ***SyRS–Dynamic Mobility Applications Open Source Application Development Portal, version 3.0*** (October 2011)[7]
  - The DMA vision document, ***Dynamic Mobility Applications Program Vision: Objectives, Core Concepts and Projected Outcomes***, located at: www.its.dot.gov/dma/dma_vision2.htm
  - A white paper titled, ***The Role of Free and Open Source Software (FOSS) and Open Data in the ITS Data Capture and Management and Dynamic Mobility Applications Program***

In addition, three policy teams have been formed to support the policy analysis and recommendations of options for the connected vehicle programs. These teams include: a Legal Policy team, a Technical Policy team, and an Implementation Policy team. Their analysis to date has informed this white paper and their continued analysis will result in recommendations for the connected vehicle mobility policies.

[7] *Task 3.3: Concept of Operations – Dynamic Mobility Applications Open Source Application Development Portal, Final Draft Document, Version 3.3.3 – August 5, 2011* (publication number and web page forthcoming) and *TASK 4.0: SyRS – Dynamic Mobility Applications Open Source Application Development Portal, version 3.0 – October 2011* (publication number and web page forthcoming).

U.S. Department of Transportation
ITS Joint Program Office-HOIT
1200 New Jersey Avenue, SE
Washington, DC 20590

Toll-Free Help Line 866-367-7487
www.its.dot.gov

FHWA-JPO-12-035

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