

# FHWA DATA GOVERNANCE PLAN

# DATA GOVERNANCE PLAN

Volume 1

Data Governance Primer

July 2015



U.S. Department of Transportation  
**Federal Highway Administration**

### **Notice**

This document is disseminated under the sponsorship of the U.S. Department of Transportation in the interest of information exchange. The U.S. Government assumes no liability for the use of the information contained in this document.

The U.S. Government does not endorse products or manufacturers. Trademarks or manufacturers' names appear in this report only because they are considered essential to the objective of the document.

### **Quality Assurance Statement**

The Federal Highway Administration (FHWA) provides high-quality information to serve Government, industry, and the public in a manner that promotes public understanding. Standards and policies are used to ensure and maximize the quality, objectivity, utility, and integrity of its information. FHWA periodically reviews quality issues and adjusts its programs and processes to ensure continuous quality improvement.

### Technical Report Documentation Page

1. Report No.	2. Government Accession No.	3. Recipient's Catalog No.	
4. Title and Subtitle		5. Report Date	
		6. Performing Organization Code	
7. Author(s)		8. Performing Organization Report No.	
9. Performing Organization Name and Address		10. Work Unit No. (TRAIS)	
		11. Contract or Grant No.	
12. Sponsoring Agency Name and Address		13. Type of Report and Period Covered	
		14. Sponsoring Agency Code	
15. Supplementary Notes			
16. Abstract			
17. Key Words		18. Distribution Statement	
19. Security Classif. (of this report)	20. Security Classif. (of this page)	21. No. of Pages	22. Price



# **DATA GOVERNANCE PLAN**

**Volume 1**

**Data Governance Primer**

**July 2015**



**TABLE OF CONTENTS**

**CHAPTER 1. DATA GOVERNANCE ORGANIZATION.....1**

**1.1 INTRODUCTION .....1**

**1.2 DATA GOVERNANCE AND STEWARDSHIP PROGRAM PLAN.....2**

Key Data Issues.....2

Goals and Objectives .....2

Success Measures.....3

**1.3 DATA GOVERNANCE WORK PLAN.....4**

Overview.....4

Organization.....4

**1.4 DATA STEWARDSHIP ROSTER.....6**

**1.5 DATA GOVERNANCE COLLABORATION .....6**

**CHAPTER 2. DATA GOVERNANCE FRAMEWORK.....7**

**2.1 DATA POLICIES .....8**

**2.2 DATA STANDARDS .....10**

Data Integrity, Sharing and Information Exchange Consistency .....10

NIEM Standards & Compliance .....11

Metadata .....12

Service Level Agreements.....12

Quality .....13

Reliability .....14

**2.3 DATA PROCEDURES.....14**

Information Architecture Life Cycle.....15

Developing Data Artifacts & Entities .....16

Enterprise Data Archive and Purge Process .....16

Enterprise Data Resolution Process .....16



**NEXT STEPS** ..... 18

**APPENDIX A - DATA GOVERNANCE ROSTERS** ..... 19

**DATA GOVERNANCE ADVISORY COUNCIL** ..... 19

**THE TECHNICAL ADVISORS** ..... 19

**APPENDIX B - DATA GOVERNANCE CHARTER**..... 21

**ARTICLE I. PURPOSE, AUTHORITY, AND DURATION**..... 21

**ARTICLE II. SCOPE AND MANDATES**..... 21

**ARTICLE III. MEMBERSHIP**..... 22

**ARTICLE IV. SCHEDULE**..... 23

**ARTICLE V. EFFECTIVE DATA AND REVIEW** ..... 23

**APPENDIX C - KEY TERMS & ACRONYMS** ..... 25



## CHAPTER 1. DATA GOVERNANCE ORGANIZATION

This section of the FHWA Data Governance Plan provides the organizational framework for how Data Governance will be managed within the Agency.

### 1.1 INTRODUCTION

This document is intended to provide a brief introduction to Data Governance and how it will be implemented within the Federal Highway Administration (FHWA). The Data Governance Plan is being created by the FHWA Data Governance Advisory Council (DGAC). DGAC is formed as an advisory council to the FHWA Investment Review Board (IRB), which is chaired by the FHWA Chief Information Officer (CIO). The DGAC's Charter (see appendix A) has established the DGAC to provide strategic review and oversight for all FHWA data collection efforts. The DGAC has the authority and responsibility to corporately advise on the utilization of FHWA's data resources and recommend necessary changes to FHWA data collection efforts that will result in;

- 1) increased consistency and coordination between existing and new data programs;
- 2) elimination of redundant data collection;
- 3) consolidation of data sources and resources;
- 4) compliance with external mandates.

This volume of the Data Governance Plan (DGP) is the first step towards achieving these goals. Future volumes of the DGP will be developed by the DGAC and presented to the FHWA IRB for concurrence and approval.

## 1.2 DATA GOVERNANCE AND STEWARDSHIP PROGRAM PLAN

The FHWA data governance and stewardship strategic goals address the issues and challenges currently confronting the organization, which hinder good business decisionmaking. These issues are at the heart of the improvements in data management desired by FHWA.

### Key Data Issues

- Finding consistent data for business needs and partner/customer inquiries.
- Identifying real and perceived data quality issues.
- Integrating data across offices.
- Identifying data that are valuable and needed to drive decisions.
- Standardizing approach to address existing data and new data needs.
- Preventing redundant data collection.
- Accessing needed data.
- Keeping current with changes in computer technology and electronic data storage standards.
- Maintaining security and accessibility so that data elements cannot be lost, corrupted, or otherwise made unavailable to users.

### Goals and Objectives

With the key data issues in mind, the DGAC established six strategic goals for the data governance effort. These goals guide the Council’s data governance activities, the implementation of data governance, and the selection of data improvement projects. The six strategic data governance goals are shown in the table below with their related objectives.

Table 1. Data Governance Goals and Objectives.

No.	Goal Title	Goal Description	Objectives
1	Leadership	Champion data solutions to ensure accountability and increase the value of data assets.	<ul style="list-style-type: none"> <li>• Promote data governance within FHWA.</li> <li>• Communicate data-related changes to all interested parties.</li> <li>• Monitor progress and ensure accountability of data governance tasks and projects.</li> </ul>
2	Quality	Oversee efforts to provide acceptable quality data that is accurate.	<ul style="list-style-type: none"> <li>• Establish a Data Quality Assurance Program.</li> <li>• Increase the accuracy and clarity of data.</li> <li>• Improve accessibility of data.</li> </ul>

3	Prioritization	Prioritize efforts to address data gaps and needs.	<ul style="list-style-type: none"> <li>Establish clear priorities to address data gaps and needs.</li> <li>Communicate priorities to FHWA business units.</li> </ul>
4	Cooperation	Facilitate cross-organizational collaboration, data sharing, and integration.	<ul style="list-style-type: none"> <li>Increase opportunities for data sharing.</li> <li>Eliminate data silos and other barriers.</li> <li>Ensure business units know the identity of Data Stewards.</li> <li>Ensure Data Stewards know the identity of Data Users.</li> </ul>
5	Flexibility	Encourage creative and innovative solutions to data needs.	<ul style="list-style-type: none"> <li>Identify innovative data solutions throughout FHWA.</li> <li>Communicate innovative solutions to Data Stewards and Data Users.</li> </ul>
6	Utilization	Improve data utilization and ease of access.	<ul style="list-style-type: none"> <li>Promote appropriate data usage throughout FHWA.</li> <li>Provide staff the means to determine the extent and availability of FHWA data.</li> </ul>

## Success Measures

The DGAC will be responsible for prioritizing the strategic goals and objectives, and developing projects and processes to achieve them. These projects and processes may be assigned to a team made up of various Subject Matter Experts (SMEs) or to individuals with the capability to complete the project or process. Projects will have timelines and expectations for decisions, recommendations, and/or deliverables designed to facilitate project completion and further the achievement of the objective. Processes will support the implementation of data governance as well as guide long-term consistency in how data are created and maintained within FHWA. To determine whether or not progress is being made toward achieving the objectives, the DGAC will establish performance measures related to each objective. These performance measures will ensure the accountability of a team or individual to produce the results assigned by the DGAC. The following table is intended to serve as an example; it presents a list of sample objectives and performance measures:

Table 2. Examples of Performance Measures.

No.	Objective	Performance Measure
1	Data meet established need-driven standards for accuracy.	% of data that meet standards.
2	Meaning of data is readily understood.	% of data elements for which clear definitions have been established.
3	Communicate data-related changes to all Data Users.	Affected users are aware of data-related changes at least 30 days before changes are implemented.

## 1.3 DATA GOVERNANCE WORK PLAN

The purpose of the Data Governance Work Plan is to establish a structured environment to ensure data quality and consistency, increase accountability and ownership of enterprise data, improve data security, and optimize usage of data for business intelligence and decisionmaking processes.

### Overview

FHWA Data Governance will be a collaborative effort involving all functional areas within the organization. The focus will be on the systems that are used to collect, store, analyze, and report the data, as well as the users and uses of the data. This is an encompassing effort that will include all business units within FHWA.

The Data Governance Plan is intended to assist in the development and maturity of pertinent data programs, including systems that reside on FHWA-owned servers that are managed by Office of Information Technology Services (OITS) staff, as well as FHWA systems hosted by external entities. Smaller staff developed databases (i.e., MS Access or MS SQL Server) residing on network drives or SharePoint may eventually be included depending on the following 1) number of people using the database, 2) size and extent of the data being stored and processed, and 3) applicability outside of the Program or Division Office. **At this time, individual or work group developed and maintained spreadsheets are not within the scope of FHWA Data Governance efforts.** The data standards and rules are identified through guidance issued via the highest authoritative federal entities. This will ensure alignment with federal business lines; however, if the rules specified from the higher levels of authority are not applicable, feasible, or specified, then the rules set by the next level of authority will be followed. FHWA Data Stewards are responsible for identifying the appropriate rules and standards and assisting the FHWA Enterprise Architecture team in developing appropriate data standards. The ultimate goal is to promote data consistency and integrity enforced across the enterprise.

### Organization

Data Governance will follow a three tiered hierarchy comprised of the functional areas:

- Data Governance Advisory Council
  - Data Governance Technical Advisors
- Data Governance Regimes & Coordinators
- Data Stewards

#### *Data Governance Advisory Council*

The Data Governance Advisory Council (DGAC) is responsible for developing the FHWA Data Governance Plan and Framework, which will serve as the foundation for developing the formal Data Governance processes and procedures for managing all existing and future data programs. The Council also will serve as the point of contact for coordinating data collection efforts with the Department, other transportation modes and other branches of government. The current list of DGAC members is available on the [Data Governance SharePoint site](#)<sup>1</sup> and in Appendix A.

<sup>1</sup> For more information visit [http://our.dot.gov/office/fhwa.policy/HPPI/Data\\_Governance/default.aspx](http://our.dot.gov/office/fhwa.policy/HPPI/Data_Governance/default.aspx)

## *Data Governance Regimes & Coordinators*

The twelve Data Governance Regimes are responsible for coordinating with the individual data programs and ensuring that the Data Governance Plan and Framework are adhered to. The coordinators are responsible for initiating changes that establish stewardship and management processes for data programs within their regime. The regimes must follow the processes and procedures established by FHWA Data Governance Council and may elect additional processes and procedures provided they include and build upon those established by the DGAC. The activities within each Regime will fall under the supervision of a Regime Coordinator. The following is a list of the Data Governance Regimes:

- Administrative
- Financial
- Operations
- Policy
- Infrastructure
- Chief Counsel
- Safety
- Research
- Federal Lands
- Division Office
- Technical Service

The Regime Coordinators are responsible for the data programs within their regime. The Coordinators serve two important functions: liaison and oversight. They serve as a liaison between the DGAC and the Data Stewards. They also serve in an oversight capacity, ensuring that the individual systems within the regime are in full compliance with the policies and standards established by the DGAC. Some regimes may determine that they need to establish some additional guidelines or procedures for the data programs in the regime. In this situation, the Regime Coordinator will also serve as the keeper and enforcer of the Regime's Data Governance Plan.

## *Data Stewards*

The Data Stewards are the subject matter experts and points of contact for the data programs they oversee. These individuals are ultimately responsible for the defining, managing, controlling, and preserving the integrity of departmental or enterprise data resources. Therefore, they are expected to manage their data systems in accordance with the processes and procedures established by the DGAC and the Regime Coordinator.

## *Data Governance Technical Advisors*

The DGAC will be assisted by Technical Advisors that will assist in developing all formal documentation and providing input into the decisionmaking process. The Technical Advisors will be comprised of staff from the Office of Information Technology Services (OITS) and the Office of Highway Policy Information (HPPI), along with a number of FHWA Data Stewards and Users. Technical Advisors will be selected based on their knowledge of FHWA data programs as well as data governance principles and best practices. The current list of Technical Advisors is included in Appendix A.

The figure below demonstrates the relationship between IRB, DGAC, Regime Coordinators, and Data Stewards. The Technical Advisors provide input and feedback directly to the DGAC. Appendix A.

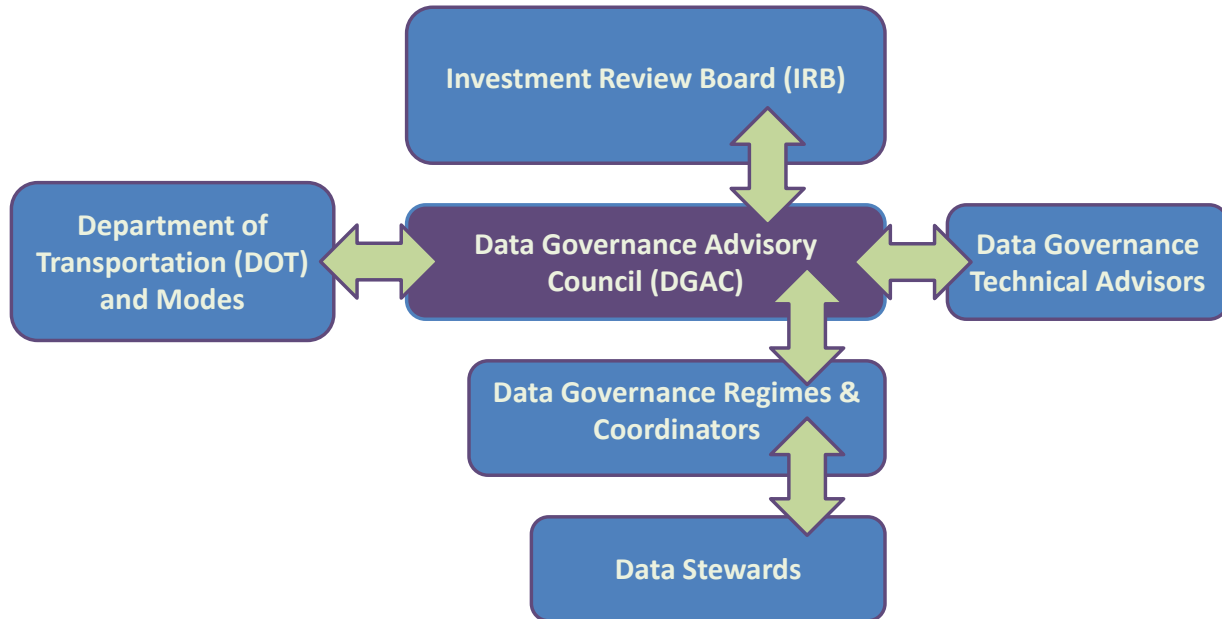


Figure 1. Chart. Data Governance Organization.

#### 1.4 DATA STEWARDSHIP ROSTER

A complete list of the individuals involved with Data Governance within FHWA will be maintained in a Data Governance SharePoint site, which will be accessible to all employees. The SharePoint site will also include the rosters for the Regime Coordinators, Data Stewards, and Technical Advisors.

#### 1.5 DATA GOVERNANCE COLLABORATION

The Data Governance SharePoint site will be used to facilitate the collaboration and storage for all artifacts generated by the DGAC. The DGAC members and Technical Advisors will all be granted full access to the site. Regime Coordinators and FHWA staff will be granted read-only access to the site. The Data Governance website (<https://www.fhwa.dot.gov/datagov>) will be used for sharing documents with US DOT and FHWA staff, and external partners and stakeholders

## CHAPTER 2. DATA GOVERNANCE FRAMEWORK

This section of the Data Governance Plan establishes the framework used by the DGAC to develop and maintain the FHWA principles of data management. It will be comprised of an operational set of data governance Policies, Standards, and Procedures used for managing and monitoring FHWA-wide data creation, collection, acquisition, quality, integrity, interoperability, and security aspects of the Enterprise Architecture.

At a high level, the Data Governance Framework describes how the DGAC proposes to manage FHWA data. The Framework will be built upon the existing data policies, standards, and procedures that are currently in use within each individual data program. While some work has been done in the past to connect data policies with standardized naming and data collection, these efforts are limited to a handful of data programs and have not been enforced at an Enterprise scale.

There is a hierarchical relationship among data policies, standards, and procedures as shown in the graphic below. Data policies are high-level statements that represent a desired state or outcome consistent with the established strategic goals and objectives. The data standards provide further detail on how the DGAC intends to implement the various policies. Many of the data standards cut across more than one data policy. Finally, the data procedures contain detailed descriptions of data rules and their application.

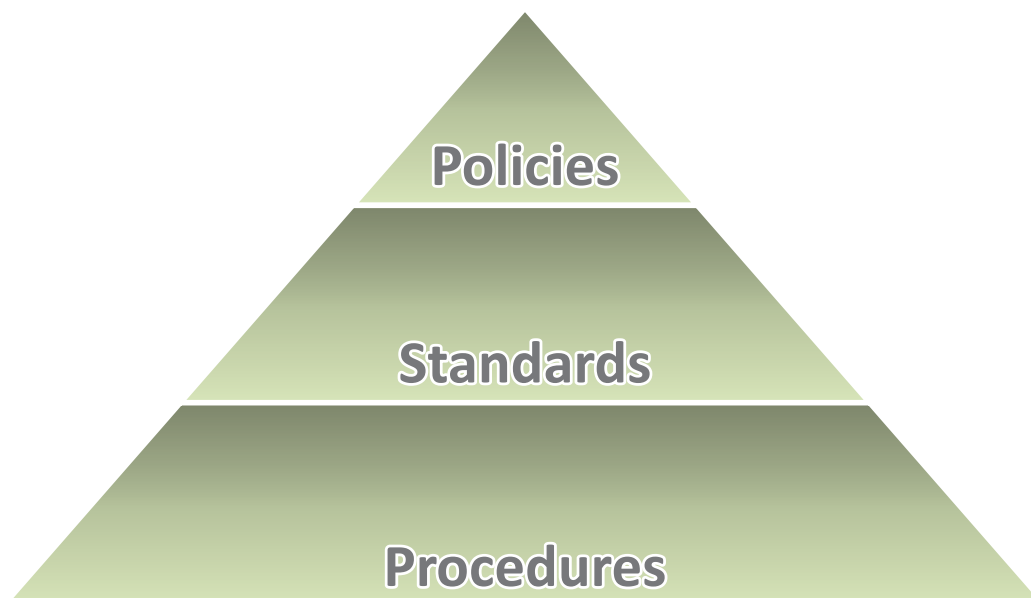


Figure 2. Chart. Data Governance Framework Hierarchy.

## 2.1 DATA POLICIES

The following Data Policies foster consistent expectations as to how data are to be treated and managed throughout FHWA. The proposed policies guide data creation, acquisition, storage, quality, integrity, interoperability, security, and privacy. Adoption of the policies ensures the successful development of procedures to identify and rectify data management deficiencies, and create a set of FHWA-wide data standards.

Table 3. FHWA Data Policies.

No.	Policy Name	Policy Description
1	FHWA data are an enterprise asset	Data, structured and unstructured, and the corresponding meta-data, are business and technical resources owned in whole or in part by FHWA. FHWA data include shared data about managed entities, interests, finances, employees, resources, customers, providers, business affiliates, best practices, operating procedures, experimental results, etc. All employees must recognize that the proper management of strategic enterprise data is critical to the success of the organization.
2	FHWA data programs and activities must undergo IT investment process	FHWA data programs or data related activities within IT projects require Investment Review Board (IRB) approval prior to and during an ongoing effort. This process is typically initiated, liaised, communicated to IT project managers, or executed by the Data Stewards. They are ultimately responsible for following the FHWA Information Technology Investment Process in order to gain IRB approval prior to and during all planned/ongoing data activities.
3	FHWA data must be consistent	All strategic FHWA data shall be modeled, named, and defined consistently, according to standards, across the organization. Efforts must be made by management to share data and not maintain redundant data without justification. Originating business stewards of data must recognize the informational needs of downstream processes and business units that may require FHWA data.
4	FHWA data must be of acceptable quality	Quality data are critical to ensuring FHWA mission success. Data Stewards are responsible for ensuring that FHWA data are accurate and correct for the intended purpose and use, and that data providers follow all reporting requirements regarding the collection, processing, and reporting of FHWA data, and meet all requirements of the <a href="#">Data Quality Act</a> . Data quality standards shall be managed and applied actively to the approved reliability levels of FHWA data as defined by the business owners.



# FHWA Data Governance Plan

5	FHWA data must be interoperable with dependent systems	All enterprise data (structured and unstructured) must conform to a common set of standards and schemas across all data sharing parties. Data sharing must also be accounted for and facilitated through a designated authority.
6	FHWA data must be maintained at the source	All FHWA data must be maintained as close to the source as feasible, to reduce the collection and storage of redundant data.
7	Enterprise data must be safe and secured	FHWA data, in all electronic formats, shall be safeguarded and secured based on recorded and approved requirements and compliance guidelines. These requirements are to be determined by the OITS. Appropriate backups and disaster recovery measures shall be administered and deployed for all FHWA data. The enterprise data must adhere to the privacy rules and requests made by each respective business steward both internal and external to FHWA.
8	FHWA data must be accessible	FHWA data, information, and meta-data shall be readily accessible to all, except where determined to be restricted. When restrictions are made, business stewards of the data are accountable for defining specific individuals and levels of access privileges that are to be enabled. The OITS will be responsible for the implementation of proper security controls.
9	Meta-data will be recorded and utilized	All FHWA information system development and integration projects will utilize the defined meta-data program for data naming, data modeling, and logical and physical database design purposes. The DGAC is responsible for developing plans to capture and record specific data administration-focused meta-data consistent with the defined meta-data program.
10	Data stewards will be accountable by job description	Individuals designated as stewards will have specific enterprise data accountabilities incorporated into their job descriptions.
11	Timeliness of data	Data must be obtained, processed and be made available in a timeframe consistent with its intended use.

## 2.2 DATA STANDARDS

The Data Standards described in this section will be applied to all new data collection efforts, as well as additions or modifications to existing data programs. Given the extent and complexity of existing data programs, the Data Standards will be initiated when one of the following trigger events occurs:

- A data program undergoes a regular or periodic reassessment that examines data utility and viability.
- New data fields are added to an existing data system.
- A data redundancy, quality, or consistency issue is identified that has led to one or more of the following:
  - Increased data collection and/or reporting burden.
  - Increased data storage and/or analysis burden.
  - Inability to perform quality data analysis or convert data into meaningful information.

### Data Integrity, Sharing and Information Exchange Consistency

FHWA data must be consistent across all domains and locations. To ensure data integrity, copies of data, static or dynamic (i.e., working data) must be uniformly stored and accessible across all platforms, systems or locations. Data should only be collected if there is a clear, unique, business requirement. Drifting from this governing policy could lead to unnecessary data collection resulting in unforeseen consequences such as definition conflict or unnecessary management overhead.

Any changes made to the data or schema must be performed in a methodical fashion. Only authorized users or systems may conduct adjustments or edits to data, after being granted proper adjudication, and by following a previously approved modification plan. The formal approval should be reviewed, granted, and documented through the Regime Coordinators, unless the changes are considered minor or have minimal impact on overall data architecture, in which case the changes can be approved and executed by staff under the guidance of Data Stewards.

The FHWA Enterprise Architecture Team will develop standards pertaining to Data Consistency and Integrity. Regime Coordinators and Data Stewards are ultimately responsible for ensuring that the data consistency and integrity standards are embedded within their systems and data implementation processes. All data exchanges shall ensure, from a high level, the following data characteristics remain consistent and unchanged.

Table 4. Data Standards.

No.	Information Characteristic	Characteristic Description
1	Names and Attributes	The variable names and associated attributes must be unique across all systems. The names may be static, or determined during system execution run-time.
2	Container Format	The FHWA content data must be accurately documented to reflect the expected character types, formats, field min/max lengths and all other format specific characteristics.
3	Content Length	All uniquely defined variables must specify reasonable data length. All mapping variables should in turn conform to the specified content length.
4	Data Definition Conformity	Data definitions must be established and specified between mapping entities and variables.
5	Schema Uniformity	All XML/Database schemas developed as the result of a cross-boundary information exchange must be uniform and conform to the developed Information Exchange Packages (IEPs).
6	Central Metadata Repository	All metadata associated with the information exchange must be stored in an agreed upon central location and accessible to all parties having a business need for access to the data.

## NIEM Standards & Compliance

National Information Exchange Model (NIEM) is a community-driven, government-wide, standards-based approach to exchanging information. FHWA highly recommends its adoption for developing data modeling schemes and interoperability. The ultimate goal is to achieve consistency, simplicity, and flexibility in information exchange throughout FHWA, Department of Transportation, and other federal agencies, as well as external entities.<sup>2</sup>

NIEM compliance can be applied to the following scenarios in exchanging data:

### *Data that exist in more than one system (cross-boundary)*

FHWA data that exist in multiple systems, platforms, or storage locations (i.e., redundant data) must follow the established consistency and reliability standards. A uniform method of defining, collecting, and storing redundant data will help overcome the data challenges associated with distributed data. To facilitate data sharing, all partnering organizations and entities are encouraged to conform to NIEM standards in developing data exchanges.

<sup>2</sup>For more information visit <https://www.niem.gov/technical/model-package-description/Pages/mpd.aspx> and <http://www.goniem.com/site/node/6>

### ***Data that exist in only one system***

Data that exist within only one system, or are in use by a close family of systems residing in an isolated platform, either belonging to FHWA or an external entity, must be consistent with FHWA naming conventions. Although not required, NIEM Information Exchange Packages Documents can still be used for exchanging data within only one system. In this scenario, the definitions must be clear, concise, and easily understood.

### ***Data that exist in external system(s)***

Variances in schemas and formats corresponding to external data may exist in any form specific to the external systems' business needs. However, the datasets shared with FHWA must conform to FHWA data rules. To accomplish that, the data exchange must follow the IEPs developed by FHWA and the entity owning the external system. Therefore, the NIEM compliant systems will easily be able to exchange information.

### **Metadata**

Metadata is defined by National Information Standards Organization (NISO) as “structured information that describes, explains, locates, or otherwise makes it easier to retrieve, use, or manage an information resource.”<sup>3</sup>

In applying standards to FHWA data programs, all data must be associated with metadata from the following three categories:

- Descriptive metadata – describes resource for data purposes such as discovery and identification. A data program undergoes a regular or periodic reassessment that examines data utility and viability.
- Structural metadata – indicates the composition of object data.
- Administrative metadata – statistical information about managing the data resource(s).

Metadata must be created by each system owner and stored in a central location for easy reference by both internal and external data users.

### **Service Level Agreements**

Service Level Agreement (SLA) is defined by The Information Technology Infrastructure Library (ITIL®) as:

“[SLA is] an agreement between an IT service provider and a customer. A service level agreement describes the IT service, documents service level targets, and specifies the responsibilities of the IT service provider and the customer. A single agreement may cover multiple IT services or multiple customers.” Administrative metadata – statistical information about managing the data resource(s).

An SLA, as defined within FHWA data governance context, aids in setting business relationships to manage shared data and information exchanges among FHWA offices and external entities.

<sup>3</sup> For more detailed information visit <http://www.niso.org/publications/press/UnderstandingMetadata.pdf>

The body of an SLA document articulates technical rules of engagement, founded on established business rules.

Formal SLAs must be established within the existing systems and operational standards, and embedded in all aspects of daily operation to ensure adequate accessibility as well as data access and usage accountability. Data shared across multiple systems or external to FHWA will require separate SLAs that specify and address the distinct requirements of data exchange interfaces. Solutions Architecture and Program Management are advised to research for existing MOUs and/or SLAs and reference within their standards prior to forming new formal agreements as such.

## Quality

The quality of FHWA data will be quantified and documented. Data quality management will be designated to FHWA Regime Coordinators through implementing an iterative/cyclical process during which continuous analysis and improvement will yield data quality that meets or exceeds established standards across the entire FHWA and all involved external entities. As shown in Figure 2, a baseline for data standards will be established during the iterations, followed by sets of quality evaluation criteria that are derived from the baseline. Then the quality of current data will be assessed and measured. Afterwards, the data quality metrics will be integrated with the data program's infrastructure and data quality will be further evaluated and measured for improvements. Once the evaluation cycle has been completed, the next iteration of data quality assessment and measurement will take place if necessary.

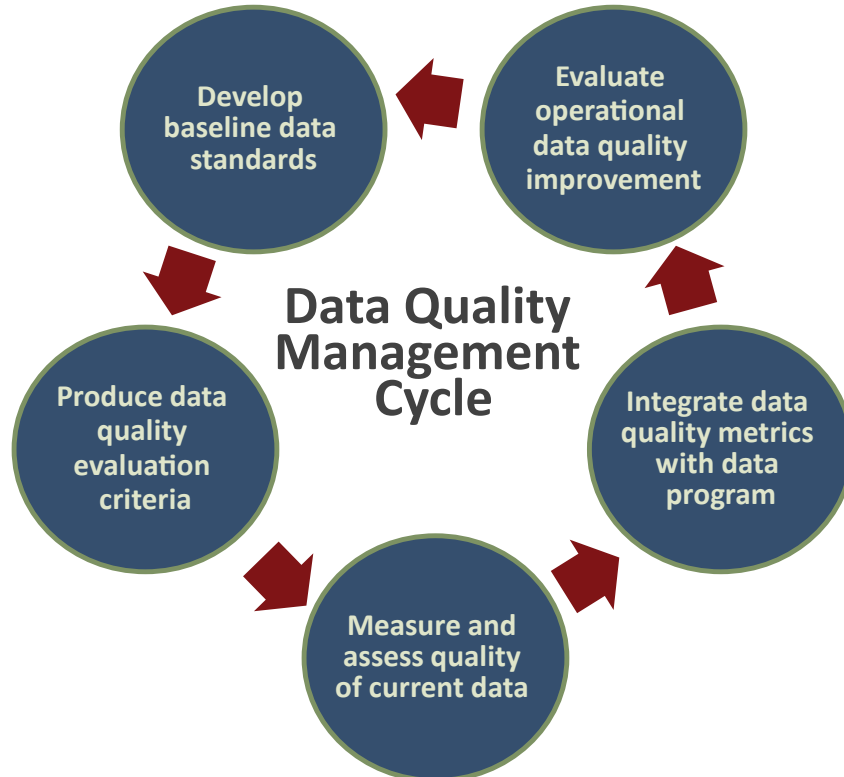


Figure 3. Chart. Data Quality Management Cycle.

In order to ensure data quality and standards across the board, FHWA's cyclical data quality method will be clearly conveyed to all partnering organizations and entities that either consume FHWA data or exchange information with FHWA, and guidance will be provided to those parties accordingly. The guidance will include the mandated as well as recommended standardized data access and manipulation methods in addition to storage technologies. FHWA data quality standards guidance will also provide data collection and reporting requirements for data that are provided by external sources.

### Reliability

FHWA data retention and access must be reliable during peak usage time, disaster events, incidents, intrusions, and all other circumstances. To achieve this goal, hosting platforms, systems and technologies must undergo an extensive Security Assessment and Authorization (SA&A) processes before data are migrated, stored, accessed, or modified on those locations. SA&A is a systematic procedure for evaluating, describing, testing, and authorizing a system or activity prior to or after a system is in operation. All FHWA data systems go through an initial and annual SA&A process. The FHWA data residing on external entities' platforms must also abide by the established reliability measures during SA&A process. FHWA is responsible for ensuring compliance.

Data Governance Technical Advisors will assist in composing a SA&A team if one does not exist for data programs, and they will provide guidance and expert knowledge in developing pertinent SA&A criteria.

## 2.3 DATA PROCEDURES

The FHWA Data Governance Framework provides guidance on the following areas across the enterprise programs:

- Controlling FHWA data creation
- Acquisition
- Quality
- Integrity
- Interoperability
- Security procedures

These procedures will be described in more detail in later chapters, which will be published and distributed within FHWA as separate volumes of the Data Governance Plan. Some procedures are expected to change as they are further developed in the near future. Listed below are highlights of the major FHWA data policies and standards-driven procedures.

## Information Architecture Life Cycle

FHWA data standards and policies must be directly mapped to the Enterprise Information Architecture and followed during each phase of the Project Management Lifecycle (PMLC), System Development Life Cycle (SDLC), and Data Lifecycle (DLC). New policies and standards are generally developed during PMLC's Planning phase, and they are applied to the SDLC and DLC during PMLC's Executing & Controlling phase.

As shown below, FHWA IT Projects tie into the SDLC and DLC through the Executing & Controlling phase of the PMLC implying that SDLC and DLC fit within that PMLC phase. Once a project reaches the Executing & Controlling phase, the Planning phase for both SDLC and DLC will begin.

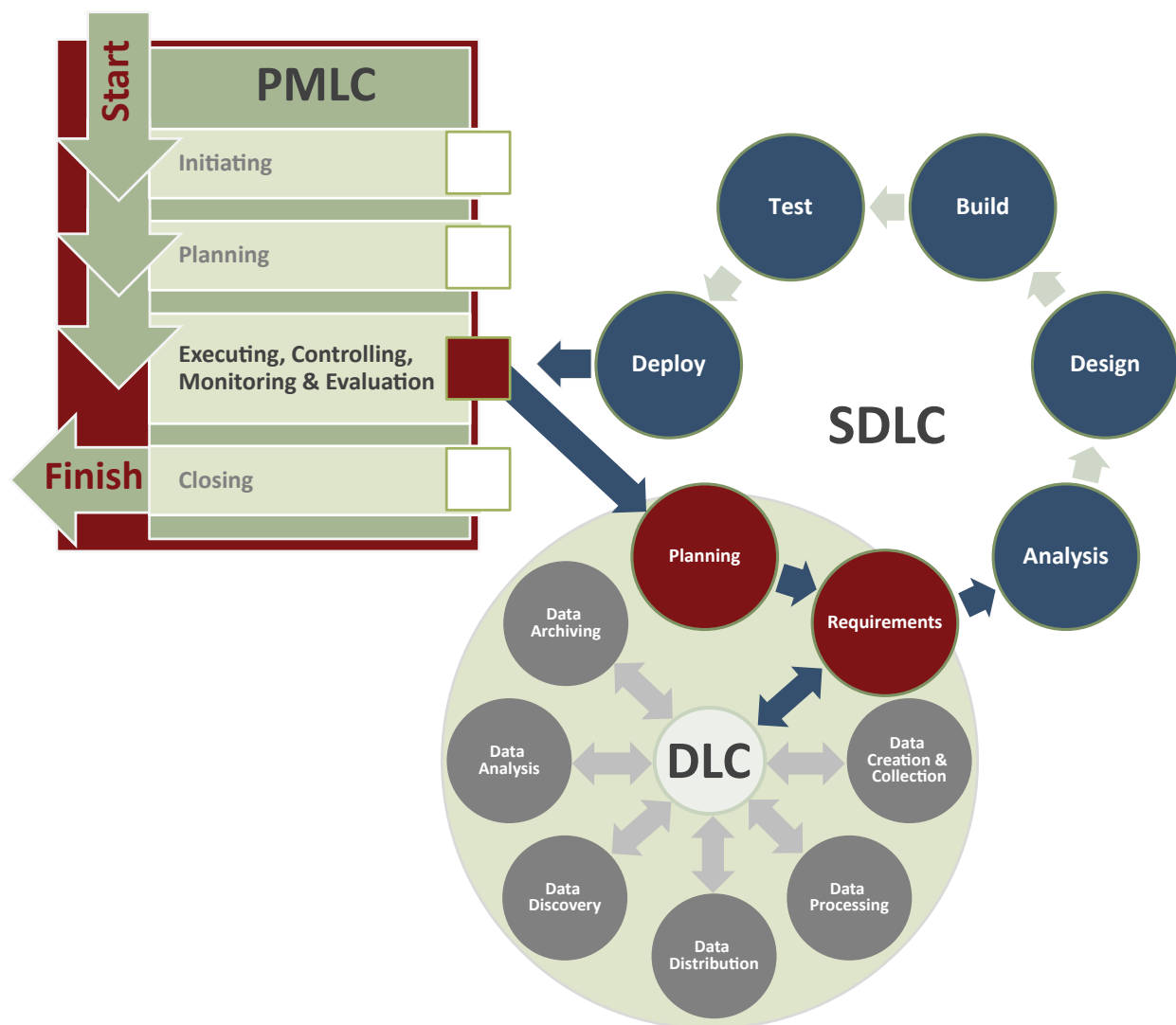


Figure 4. Chart. Information Architecture Life Cycle.

The SDLC and DLC's Planning phase is the starting point in the Systems and Data lifecycles. They run in parallel to prepare for SDLC/DLC Requirements phase. Once the SDLC/DLC Planning phase has been successfully completed, the Requirements phase for both cycles will begin.

During the Requirements phase, the new Business and Functional Requirements for the existing Architecture, Standards, and Policies are developed, in addition to those which were developed during PMLC's Planning phase.

After the SDLC/ DLC Planning and Requirements phases, the subsequent SDLC phases will continue in a spiral fashion, while each DLC phase is initiated and utilized according to the relevant requirements that were determined during the Requirements phase. Therefore, DLC phases can occur in any number or order. For example, upon establishing certain requirements, a project may entail activities under Data Creation & Collection as well as Data Processing and Data Analysis. The goal is for each activity within those DLC steps to properly map to their corresponding business and functional requirements in a Requirements Traceability Matrix (RTM).

### **Developing Data Artifacts and Entities**

Development of data artifacts and entities for Conceptual, Logical, Physical, and Security Models is driven by the FHWA Data Policies and Standards. These models depict the large scale views or an overview of data entities such as XML Schemas and database objects, their inter-relationships and overall relevance to the Enterprise Information Architecture. Data Artifacts support database and software development by providing documentation about the development process, and generally include data entity relationship diagrams, data dictionaries, UML class diagrams etc. These artifacts reveal the data components of the overall enterprise programs, from a larger perspective. These products must also be accompanied by taxonomy standards in order to uniformly identify FHWA data concepts, entities, definitions, and attributes.

### **Enterprise Data Archive and Purge Process**

FHWA programs must follow the US DOT's departmental guidelines as well as Office of Management and Budget's and Executive Branch Administration's policies and standards for the methods and appropriateness of data archiving and purging. The methods and procedures applied to archiving shall be aligned with policies controlling quality, context, availability, and security aspects of retaining data that are not in active use. Disposal of FHWA data requires a thorough justification by the data program managers, followed by a formal request to the appropriate Data Stewards to obtain data purging approval. Data Stewards are encouraged to consider all options in retaining the data before agreeing to dispose of data permanently, especially in case of disposing of metadata or other references to external sources of information.

### **Enterprise Data Resolution Process**

Ideal data architectures require minimal redundancy to support simultaneous operation of multiple data applications without conflict. Since achieving the ideal state is virtually impossible, a Conflict Resolution Process (CRP) is required to ensure smooth business



operations. The Regime Coordinators provide oversight for CRPs and the data stewards are responsible for preventing and mitigating data discrepancies or potential conflicts within their entrusted data architecture. Any data conflict beyond the data architecture boundaries is outside the intended scope of this document.

## *Conflict Resolution Process Description*

Conflicts can occur during the data lifecycle. Therefore, it is highly recommended that the standards and responsibilities for capturing and resolving data issues are to be identified during the DLC/SDLC's Planning phase and continually refined during the PMLC's Evaluation phase.

The Conflict Resolution Process must focus on three main areas: Conflict Prevention, Conflict Detection, and Conflict Resolution. It must also comply with the Federal Enterprise Architecture Framework and adequately describe the data issue resolution process in full detail, guide the execution of the process, and facilitate communication throughout the Administration.

## *Major Initiatives Timelines*

The major Data Governance activities are summarized and structured in a certain parallel fashion as depicted in Figure 5.

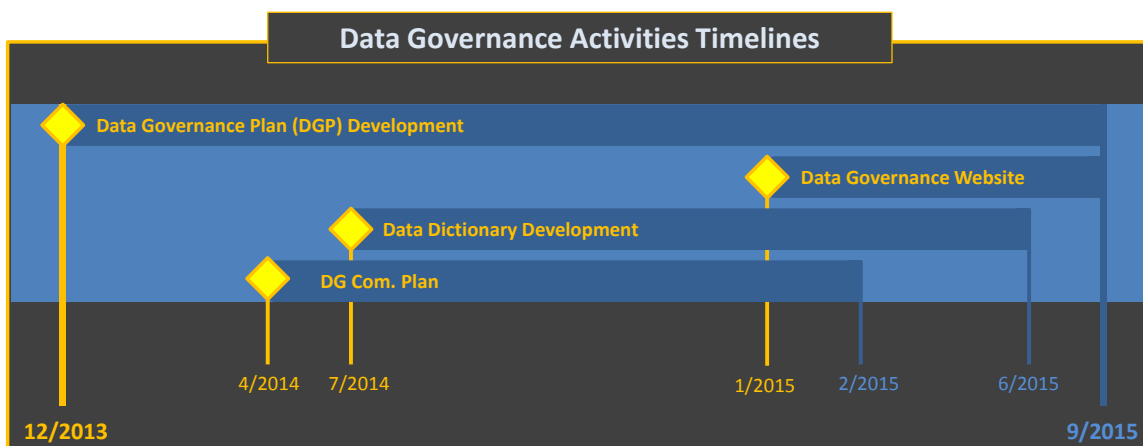


Figure 5. Major Data Governance Timelines.

## NEXT STEPS

As previously mentioned, this document is the first of six planned volumes which together comprise the FHWA Data Governance Plan. Following the completion and dissemination of this volume, the DGAC and the Technical Advisors will begin drafting the remainder of the Data Governance Plan. The remaining five volumes are as follows:

### **VOLUME 2: ENTERPRISE ARCHITECTURE**

- Chapter 3 – Enterprise Data Architecture Landscape (As-Is)
- Chapter 4 – Enterprise Data Strategy (To-Be)
- Chapter 5 – Enterprise Data Architecture Work Plan

### **VOLUME 3: DATA ANALYTICS AND STORAGE**

- Chapter 6 – Business Intelligence and Data Warehousing Business Case Analysis
- Chapter 7 – Meta-data Work Plan

### **VOLUME 4: MASTER REFERENCE DATA**

- Chapter 8 – Data Program Meta-data
- Chapter 9 – Data Dictionary

### **VOLUME 5: OPEN DATA**

- Chapter 10 – Open Data Action Plan

### **EXECUTIVE SUMMARY**

Following the successful dissemination of each volume in the Data Governance Plan, the DGAC will undertake a series of educational and promotional activities to inform and educate FHWA staff and as appropriate, non-FHWA partners and stakeholders. The development of the Data Governance Plan is likely to span several years, and is therefore subject to change based on a wide variety of internal and external factors. Deployment and implementation of the Data Governance Plan will likely take several additional years.

## APPENDIX A - DATA GOVERNANCE ROSTERS

### DATA GOVERNANCE ADVISORY COUNCIL:

- David Winter – Highway Policy Information
- Brian Bezio – Office of Chief Financial Officer
- Seetha Srinivasan – Chief Counsel Office
- Scott Johnson – Policy and Program Review, Federal Lands Highway
- Philip Yen – Bridge and Structures
- Peter Stephanos – Transportation Performance Management
- Michael Griffith – Safety Programs
- Cheryl Richter – Research, Development and Technology
- Renee Sigel – DA Council
- Kevin McLaury – IT Advisory Group
- Robert Arnold – Operations
- Robert Bini – Planning, Environment, and Realty

### THE TECHNICAL ADVISORS:

- Joel Askland – Western Federal Lands
- Walter During – Operations
- Tom Everett – Bridge and Structures
- Nila Fridley – Information Technology Services
- Danny Jenkins – Highway Policy Information
- Jane Jiang – Research, Development and Technology (Pavement)
- Donna Jones – Office of Chief Financial Officer
- Sonia Juneja – Information Technology Services
- Lloyd Rue – Montana Division
- Aramis Lopez – Research, Development and Technology (Pavement)
- Jim McGrath – Information Technology Services
- Stephen Perry – Information Technology Services
- Tom Roff – Highway Policy Information
- Heather Rothenberg – Safety
- Robert Rupert – Operations
- Wes Rutland-Brown – California Division
- Tim Schmidt – Research, Development and Technology (IT)
- Carol Tan – Research, Development and Technology (Safety)
- Ralph Volpe – Resource Center
- Eric Weaver – Research, Development and Technology (Pavement)



## APPENDIX B - DATA GOVERNANCE CHARTER

The following Charter was signed by Sarah J. Shores, Associate Administrator for Administration and David R. Winter, Director, Office of Highway Policy Information, on December 1, 2012.

### ARTICLE I. PURPOSE, AUTHORITY, AND DURATION

**Purpose:** The Federal Highway Administration (FHWA) Data Governance Advisory Council, hereinafter referred to as the “DGAC,” is formally chartered and empowered to provide strategic review and oversight of all FHWA data collection efforts. The DGAC will consider guidance and information provided by the DOT Secretary, the FHWA Administrator and the FHWA Chief Information Officer (CIO) as part of its processes and functions. The DGAC has authority and responsibility to corporately advise on the utilization [of] FHWA’s data resources and recommend major changes in FHWA data collection efforts that will result in increased consistency and coordination between existing and new data programs; the elimination of redundant data collection; the consolidation of data sources and resources; and compliance with external mandates. The DGAC will present recommendation to the Investment Review Board (IRB) for approval and prioritization.

**Authority:** The Council is formed under delegated authority from the Secretary of the DOT and FHWA Administrator, and in support of the Department’s implementation of the following laws:

- The Clinger-Cohen Act of 1996
- Federal Acquisition Streamlining Act of 1994 (FASA)
- Federal Information Security Management Act of 2002 (FISMA)
- E-Government Act of 2002 (E-Gov Act)
- Paperwork Reduction Act of 1995 (PRA)
- Government Performance and Results Act of 1993 (GPRA)

The DGAC is also formed to assist in the Agency’s compliance with various regulatory, policy, or procedural requirements of the OMB, and the DOT.

**Duration:** The DGAC is considered a permanent FHWA governance body.

### ARTICLE II. SCOPE AND MANDATES

**Scope:** The DGAC is an Agency-level, senior leadership governance committee whose scope includes:

- Corporately provide advice on the management of FHWA data assets.
- Provide recommendations on FHWA strategic data decisions and resource allocations to the FHWA leadership to obtain initial approval of data policies and standards.
- Annually review the FHWA data programs and make change recommendations to the FHWA Investment Review Board (IRB) for approval.

**Mandates:** The DGAC shall be responsible for orchestrating FHWA's major data collection efforts, including the pre-selection, selection, control, and evaluation of individual data and entire data programs.

In addressing these stages, the DGAC shall perform the following functions:

- Develop a proposed plan for corporately managing FHWA data.
- Review existing data collection efforts for need, consistency and efficiency annually.
- Review and approve all new data collection efforts, including the establishment and approval of criteria.
- Monitor and evaluate performance of data programs.
- Creation of a functional data dictionary.
- Recommend to the FHWA Investment Review Board ways to improve and streamline existing and new data collection efforts.
- Coordinate FHWA data collection efforts with other modes within the Department.

### **ARTICLE III. MEMBERSHIP**

**Membership:** The FHWA DGAC membership includes the following senior managers or their designees, who are all voting members:

- Director of the Highway Policy Information, who serves as the Chair
- Representative from the Office of the Chief Financial Officer
- Representative from the Chief Counsel Office
- Representative from the Policy and Program Review, Federal Lands Highway
- Representative from the Office of Bridge and Structures
- Representative from the Transportation Performance Management
- Representative from the Safety Programs
- Representative from the Research, Development and Technology
- Representative from the DA Council
- Representative from the IT Advisory Group
- Representative from a Program Office that will rotate on an annual basis

Note: Only one representative from each office is permitted.

## **ARTICLE IV. SCHEDULE**

The DGAC will meet regularly at a time and place set by the Chair. The DGAC will meet at least once each quarter.

## **ARTICLE V. EFFECTIVE DATA AND REVIEW**

This charter is effective as of December 1, 2012. There are no cancellations associated with the implementation of this DGAC Charter.





## APPENDIX C - KEY TERMS & ACRONYMS

Table 5. Key Terms & Acronyms.

Term (Acronym)	Definition
Security Assessment and Authorization (SA&A)	The process by which Federal agencies are required to apply a process of formal assessment, testing, and acceptance of system security controls that protect information systems and data stored in and processed by those systems.
Chief Information Officer (CIO)	An executive role that provides IT policies, maintains IT infrastructure within the organization, ensures proper security measures are followed, and evaluates and controls capital expenditures to facilitate the portfolio management of the organization.
Conflict Resolution Process (CRP)	A methodical process during which [data] conflicts between two systems and/or entities are resolved.
Data Governance Advisory Council (DGAC)	DGAC is a formally chartered and empowered council that provides strategic review and oversight of all FHWA data collections and efforts.
Data Life Cycle (DLC)	DLC is a policy-based approach to managing the flow of an information system's data throughout its life cycle.
Federal Acquisition Streamlining Act (FASA)	Streamlines the Federal government's acquisition system and dramatically changes the way the government performs its contracting functions, and strongly states preference for buying commercial off-the-shelf items, rather than purchasing through the detailed bidding process for custom made items.
Federal Highway Administration (FHWA)	A Department of Transportation mode that coordinates highway transportation programs in cooperation with states and other partners to enhance the country's safety, economic vitality, quality of life, and the environment.
Federal Information Security Management Act (FISMA)	United States legislation that defines a comprehensive framework to protect government information, operations and assets against natural or man-made threats.
Government Performance and Results Act (GPRA)	United States Law, enacted in 1993 to improve government project management, as it requires agencies to engage in project management tasks such as setting goals, measuring results, and reporting their progress.
Information Exchange Package (IEP)	An XML based information exchange framework that represents a collaborative partnership of organizations across United States government agencies and the private sector.
Information Exchange Package Document (IEPD)	Documentation pertaining to a given Information Exchange Package (IEP).

Investment Review Board (IRB)	Business systems investment review process that provides a governance and oversight framework for effective decision making on investments, and to enable the FHWA’s leadership in maximizing the overall impact of those investments.
Information Technology Infrastructure Library (ITIL)	A set of practices for IT service management (ITSM) that focuses on aligning IT services with the needs of the business.
Memorandum of Understanding (MOU)	A bilateral or multilateral agreement between two or more parties. It expresses a convergence of will between the parties, indicating an intended common line of action.
National Information Exchange Model (NIEM)	NIEM initially started within the justice and homeland security communities as a way to produce a set of common, well-defined data elements for data exchange and harmonization. It has since been expanded to cover all areas of government.
National Information Standards Organization (NISO)	A US non-profit standards organization that develops, maintains and publishes technical standards related to publishing, bibliographic and library applications.
Requirements Traceability Matrix (RTM)	A document, usually in the form of a table, which correlates any two baseline documents that require a many-to-many relationship to determine the completeness of the relationship.
System Development Life Cycle (SDLC)	A term used in systems engineering, information systems and software engineering to describe a process for planning, creating, testing, and deploying an information system.
Service Level Agreement (SLA)	An agreement between two or more parties, where one is the service provider and the others the customers.
Subject Matter Expert (SME)	A person who is an expert in a particular area or topic.
Extensible Markup Language (XML)	A markup language that defines a set of rules for encoding documents in a format that is both human-readable and machine-readable.



