



Office of the Chief Information Officer

# Information Resources Management Strategic Plan

*FY 2007 - 2012*

# TABLE OF CONTENTS

<b>Executive Summary .....</b>	<b>3</b>
<b>GOAL Departmental IT Solutions.....</b>	<b>8</b>
<b>GOAL Enterprise Architecture.....</b>	<b>11</b>
<b>GOAL Governance .....</b>	<b>12</b>
<b>GOAL Systems Security and Privacy.....</b>	<b>14</b>
<b>GOAL Workforce .....</b>	<b>20</b>
<b>APPENDIX 1: Management Challenges .....</b>	<b>23</b>
<b>APPENDIX 2: List of Acronyms.....</b>	<b>26</b>

# Information Resources Management Strategic Plan FY 2007 - 2012

## *Executive Summary*

The Department of Transportation's top priorities are to provide fast, safe, efficient, and convenient transportation at the lowest cost consistent with those and other national objectives, including the efficient use and conservation of the resources of the United States. DOT relies heavily on the use of IT to accomplish these priorities. DOT invests more than \$2.5 billion each year on IT to carry out its mission and programs. DOT's investment in IT is important to both sustain the nation's transportation system and make it safer.

The DOT Chief Information Officer (CIO) is the principal adviser to the Secretary, and to the DOT's Operating Administrations (OA), on matters involving IT, portfolio management, and has primary DOT oversight responsibility for all departmental IT investments. As such, the CIO provides leadership to ensure that all IT investments support the strategic goals of DOT. The CIO, in conjunction with the IT governance processes, leads, coordinates, and supports key IT initiatives within and across the OAs. The CIO also coordinates and articulates a shared vision and enterprise perspective among DOT's information activities, champions Departmental initiatives to effectively manage information and provide for enterprise solutions that add value to the businesses of DOT. To that end, this DOT Information Resources Management (IRM) Strategic Plan has been prepared.

Looking to the future, DOT acknowledges that the demand for data and services will grow. In order to manage this growth, DOT will continue to streamline and improve how citizens and business partners interact with DOT. Further, DOT will utilize a Department-wide governance structure to maintain long-range strategic planning and a disciplined budget process as the basis for efficient management of a portfolio of IT investments. This enhances DOT's

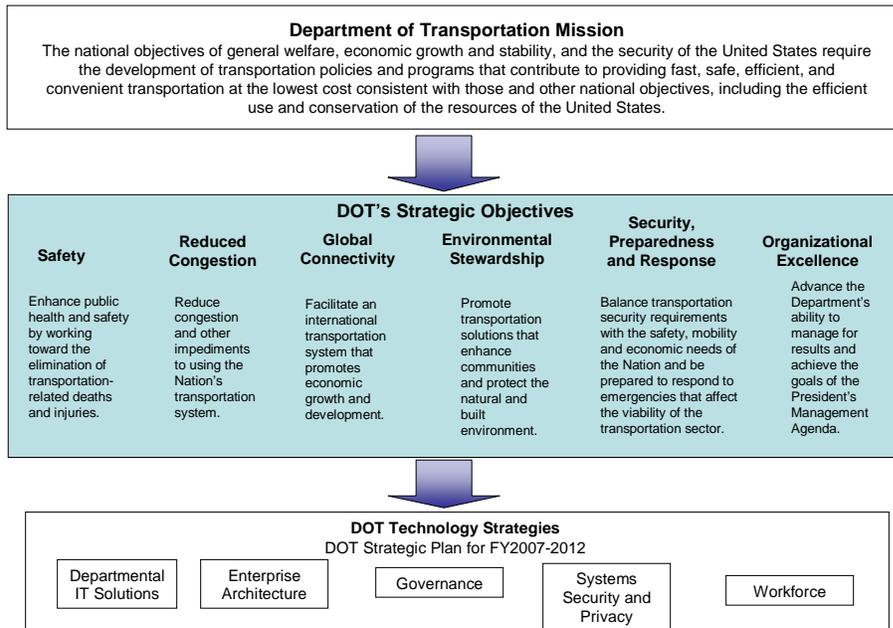
ability to address the agency mission and performance goals with the lowest life-cycle costs and least risk.

DOT's FY 2007– FY 2012 IRM Strategic Plan identifies the strategies and integrated management frameworks DOT will implement to support its strategic goals and the President's Management Agenda (PMA) and the measures of success for these goals. The DOT IRM Plan identifies guiding principles, strategic goals and major IT management activities DOT will undertake to ensure the strategies are implemented in an efficient and effective manner. This integrated approach to IT strategic planning ensures that DOT's investments in IT support DOT's overall e-Government and Lines of Business efforts to improve services to citizens, simplify business processes, and improve DOT's overall interactions with its customers.

In addition to this internal focus, DOT recognizes the need to integrate external policy directions as defined by Congress and the Administration into its IT initiatives. The DOT IRM Strategic Plan responds to the legislative mandate in the Clinger-Cohen Act of 1996 (CCA) which "...requires each agency to undertake capital planning and investment control by establishing a systematic process for maximizing the value, and assessing and managing risks of IT acquisitions of the executive agency." The Paperwork Reduction Act of 1995 specifies that agencies shall "...develop and maintain a strategic information resources management plan that shall describe how information resources management activities help accomplish agencies' missions." The Government Performance and Results Act (GPRA) of 1993, which specifies the strategic planning context and performance metrics to measure accomplishment against strategic goals, further clarifies this legislative direction. Finally, in accordance with OMB Circular A-130, this IRM Strategic Plan further supports DOT's strategic direction.

The DOT IRM Strategic Plan communicates IT Goals that link to the DOT Strategic Plan, thereby ensuring technological support to the accomplishment of DOT's critical mission requirements. DOT annual performance goals and measures serve to manage progress towards DOT's strategic objectives. They also provide the baseline performance indicators for how well IT supports DOT and its programs. DOT uses these performance indicators and measures to improve strategies and resource decisions. Figure 1 on the next page illustrates these strategic linkages.

## DOT is supporting organizational improvement and business transformation



*Figure 1 DOT Strategic Linkages*

## The IRM Strategic Plan 2007-2012 Highlights

### **Vision**

The strategic vision for Office of the Chief Information Officer for DOT is to:

*Promote the effective use of technology to enable safer, simpler, smarter transportation solutions by maximizing available resources and optimizing operations.*

### **Mission**

The mission of the Office of the Chief Information Officer for DOT<sup>1</sup> is to:

*Serve as principal advisor to the Secretary on matters involving information resources and information management, and as such, provide leadership in a visionary and collaborative manner to leverage Information Technology (IT) resources in order to improve business processes and accomplish strategic Department of Transportation (DOT) mission, goals and program objectives.*

### **Strategic Goals**

*Departmental IT Solutions:* Improve the ability to provide cross-cutting integrated IT solutions to meet the Departmental mission and business needs.

*Enterprise Architecture (EA):* Establish the EA as the authoritative decision tool for all DOT IT investments.

*Governance:* Improve governance to increase Information Technology's value to business and clarify roles and responsibilities.

*Systems Security and Privacy:* Improve critical infrastructure, networks, and information from cyber-security events that disable or significantly degrade Departmental services.

*Workforce:* Provide a world-class IT workforce for DOT.

### **How to read this plan**

The sections that follow are divided by goal and each provides the context, desired results, anticipated actions, and external factors affecting goal performance. Each goal section opens with a short narrative that establishes the context for the goal. After each goal statement, outcomes are listed establishing what will improve as a result of accomplishing the goal. Following the outcomes, a series of strategies tells how the OCIO will achieve the goals and outcomes. Finally, performance indicators and representative measures establish the foundation for tracking progress toward achieving the goals and outcomes. Also included in each goal section are external factors that may influence the OCIO's ability to achieve the goal. External factors

---

<sup>1</sup> As stated in DOT Order 1100.16, Office of the Secretary, April 23, 1997.

may be economic, demographic, social, or environmental. Finally, management challenges, or potential operational obstacles in implementing strategy, are described in Appendix 1.

## GOAL Departmental IT Solutions

### Introduction

DOT's internal and external customer requirements are increasingly complex and multifaceted in that more and more of them call for seamless access to information and data that originates from multiple sources throughout the Department. Accordingly, DOT is using the IRM Strategic Plan to increase its focus on improving capabilities and coordination in the Office of the Secretary (OST) and Operating Administrations (OAs) to be able to develop integrated information technology solutions across the DOT enterprise.

**Departmental IT Solutions Goal:** Improve the ability to provide shared services to meet the Departmental mission and business needs.

### Outcomes

1. Full lifecycle funding for IT solutions.
2. Reduced total cost of ownership.
3. Increased customer satisfaction.

### Strategies

1. Implement requested solution, on time and within budget and with minimal disruption, while maintaining and/or increasing functionality.
2. Monitor ROI targets throughout implementation of selected solutions.
3. Utilize Project Management best practices.
4. Implement shared services that are secure and accessible.
5. Establish policy and life cycle processes associated with implementing Departmental shared services and infrastructure.
6. Ensure governance bodies are empowered with the authority to commit funds as appropriate.
7. Establish full lifecycle funding for IT solutions.
8. Develop and execute a communication plan to ensure linkage between Congressional and OMB goals and Departmental IT solution implementation.

## Performance Indicators

Outcome	Performance Indicator
Full lifecycle funding for IT solutions.	Percentage and/or Number of funding requests included in the fiscal year FY2008 and in FY2010 budget.
Reduced total cost of ownership.	Number of investments that meet cost, schedule, and performance goals at quarterly reviews.
Increased customer satisfaction	Percentage of customer requirements met from a FY2008 baseline of 5 shared services tracked.

*Table 1: Performance Indicators for Departmental IT Solutions*

### External Factors

External factors that influence the development of Departmental IT solutions include:

- Federal law and guidance that require agencies to plan, implement, and manage IT resources at an enterprise level, and to leverage existing and new solutions within and between agencies whenever possible. This includes the Government Performance Reform Act of 1992, E-Government Act of 2002, and OMB Circulars A-11 and A-130.
- Customer requirements for seamless access to DOT information, regardless of source within a particular area of DOT or other Federal agencies. Customer experiences with other e-government and e-commerce capabilities (e.g., Grants.gov; Google, Amazon, and eBay) set expectations for the level of capability that on-line IT services from DOT should meet.
- New information technologies are continuing to emerge in the commercial marketplace that makes on-line collaboration and information sharing easier and less expensive.
- Limits on the availability of Federal funds for DOT programs forces the Department to seek collaborative, reusable IT solutions.
- Limits on the availability of Federal funds for DOT programs forces the Department to seek collaborative reusable IT solutions.

## GOAL Enterprise Architecture

### Introduction

EA is a sound way of approaching the management of organizations and their ability to respond to changing environments and requirements. In order for DOT to position itself to make informed, justifiable decisions regarding the future investments of the Department, EA must be utilized as a decision making tool to provide answers to business questions in areas pertaining to strategic planning, business processes, data, applications, and technology to:

- support business plan development;
- identify areas of duplication and inefficiencies within Modes and across the Department; and,
- Select top priorities for Department-wide implementation and management.

The Office of Management and Budget developed the Federal Enterprise Architecture (FEA), a business-oriented framework for government wide improvement, to transform the government into one that is citizen centered, results oriented, and market based. The outcome of this effort will be a more customer-focused government that maximizes technology investments to better achieve mission outcomes. The foundation is the Business Reference Model, which describes the government's Lines of Business and its services.

**Enterprise Architecture Goal:** Establish the EA as the authoritative decision tool for all DOT IT investments.

### Outcomes

1. Reduced total cost of ownership.
2. Compliance with OMB's FEA.

### Strategies

1. OCIO validates that investments conform to the EA.
2. Communicate value to executive leadership and stakeholders. (Convince modal leadership that EA and strategies are valid and worthwhile).
3. Develop the usefulness of the EA Lines of Business, and its use is measurable (e.g., documented use is available in IRB meeting minutes, business case justification, etc.).

4. Develop a mature EA that includes a robust repository that contains the current official record for the following EA artifacts:
  - i. “As-is” or current baseline.
  - ii. “To-be” or future EA.
  - iii. Transition Plan or “roadmap” (for rationally moving from the “as-is” to the “to-be”).
  - iv. All IT documentation (e.g., processes, procedures, protocols, standards, working agreements, etc.) necessary for IT investments to perform at a DOT-agreed upon level of performance (level also to be documented).
5. Identify duplicative systems and develop transition plan for each.
6. Adopt best business practices.

### Performance Indicators

Outcome	Performance Indicator
Reduced total cost of ownership	Number of FY 2008 duplicate systems identified in the transition strategy eliminated.
Compliance with OMB’s FEA	Improved scores on external assessments

Table 2: Performance Indicators for Enterprise Architecture

### External Factors

Much of the direction for implementing Enterprise Architecture (EA) at DOT stems from the requirements set forth by the Office of Management and Budget (OMB) – “*To transform the Federal government to one that is citizen-centered, results-oriented, and market-based, the Office of Management and Budget (OMB) is developing the Federal Enterprise Architecture (FEA), a business-based framework for government-wide improvement.*”<sup>2</sup> This effort began in 2002; over time, OMB has issued successively more detailed information about how agencies are to use EA.

<sup>2</sup> <http://www.whitehouse.gov/omb/egov/a-1-fea.html>

## GOAL Governance

### Introduction

DOT is currently composed of the Office of the Secretary of Transportation and 11 operating administrations and bureaus, each with its own management and organizational structure. Effectively linking the various modes of transportation as well as meeting the requirements of the e-Gov Act of 2002 to simplify services to citizens across organizational entities will require increased levels of coordination and cooperation. There are two main governing boards that collectively address DOT IT governance requirements – the Investment Review Board and the CIO Council.

The governance structure is critical to the success of all DOT IT initiatives. Through the governance process, IT will continue to use common areas of agreement to create forums where individual modalities' interests are considered into a federation of IT initiatives. The value of this structure will be evidenced in the efficiency and cost effectiveness achieved when each IT initiative undertaken demonstrates some agreeable set of common standards in developing, managing, implementing and performance reporting. With time, this goal will evolve and sharpen to improve business delivery through IT.

At a glance, the process seems like an arduous task; however, creating a strong IT governance framework that incorporates innovative technological processes through collaborative forums will prove to be worthwhile.

**Governance Goal:** Improve governance to increase Information Technology's value to business and clarify roles and responsibilities.

### Outcomes

1. Improved customer satisfaction with the governance process.
2. Reduced risk to mission and business performance.
3. Improved compliance with appropriate Federal laws, regulations, and standards.

### Strategies

1. Ensure governance bodies are empowered with the authority to commit funds as appropriate.
2. Achieve return on IT investments that span the enterprise.
3. Improve decision-making process.

4. Define and communicate collaborative governance processes (i.e., reviewing/monitoring/evaluating, selecting/terminating, control, and appeal).
5. Develop, implement, and evaluate review process to determine customer satisfaction with the current governance process (i.e., funding source).
6. Determine criteria for evaluating IT investments to achieve measures for return on investments, risk, and performance.
7. Establish process to determine funding for enterprise IT solutions.
8. Establish roles and responsibilities for all IT governance bodies.

### Performance Indicators

Outcome	Performance Indicator
Improved customer satisfaction with the governance process.	Percentage of decisions made within established governance process.
Reduced risk to mission and business performance.	Number of investments that meet cost, schedule, and performance goals at quarterly reviews.
Improved compliance with appropriate Federal laws, regulations, and standards.	Percentage of compliance issues from previous quarter remediated on schedule.

*Table 3: Performance Indicators for Governance*

### External Factors

Much of IT governance in the federal government is prescribed and constrained by laws, regulations, and policies enforced by Congress and OMB. Compliance with these prescriptions and constraints is mandatory and must underlie and inform all IT governance activities.

## GOAL Systems Security and Privacy

### Introduction

DOT recognizes the strategic value of its data and information and strives to create a secure environment for the protection of all of its systems which manage information. Our citizens, stakeholders and the DOT community must have confidence that critical data/systems are protected and that privacy information is safeguarded. DOT endeavors to sustain and maximize a high performing environment. This will be accomplished by having a robust Information Systems Security Program to ensure reliability, availability, confidentiality and integrity of the agency's vital information/data assets.

The Information System Security Program, managed by the Department's Chief Information Officer (CIO), provides policy, technology, processes and techniques that ensure one of the best cyber protection in the federal government. This program also includes continuous system security monitoring and scanning to protect and react to security breaches and vulnerabilities.

The CIO is responsible for protecting complex and widespread information assets that are critical to achieving its Strategic Plan for FY 2007-2012. These critical systems include several major systems that are key to the national critical infrastructure. We strive to maximize the value of our assets and manage the risk associated with information technology. This means that DOT must be vigilant and obviate any risks to the system(s) and data confidentially as a part of its standard business practice.

**Systems Security and Privacy Goal:** Improve critical infrastructure, networks, and information from cyber-security events that disable or significantly degrade Departmental services.

### Outcomes

1. Zero cyber events which degrade the DOT critical infrastructure and Departmental business systems.
2. Achieved a level of protection of sensitive information that is in full compliance with Federal mandates.
3. Institutionalized procedures and training for security.

## Strategies

1. Develop an analysis of capabilities to exploit DOT cyber vulnerabilities.
2. Conduct cost benefit analysis (including attention to ROI) on unified Information Assurance solutions.
3. Assess customer satisfaction.
4. Achieve Information Assurance targets into performance plans.
5. Standardize techniques, methods, technologies, process and procedures based on best practices.
6. Develop communication and change management plans.
7. Conduct Information Assurance organizational assessment.
8. Build Department-wide cyber situational awareness capability.
9. Identify/assess cyber-training, education, and awareness gaps.
10. Improve response to cyber situations.

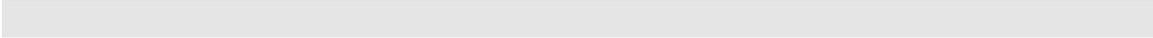
## Performance Indicators

Outcome	Performance Indicator
Zero cyber events which degrade the DOT critical infrastructure and Departmental business systems.	Number of U.S. CERT reportable events that degrade the DOT critical infrastructure or Departmental business systems.
Achieved a level of protection of sensitive information that is in full compliance with Federal mandates.	Percentage of privacy compliance issues from previous quarter remediated on schedule.
Institutionalized procedures and training for security	Percentage of users trained in DOT security procedures.

*Table 4: Performance Indicators for Security*

## **External Factors**

FISMA, the Homeland Security Presidential Security Directives, and external assessments typify the rapidly changing requirements/mandates in the security arena. DOT must respond appropriately to this fluid environment.



## **GOAL Workforce**

### **Introduction**

People are our most important asset. In IT strategy, we recognize that human capital is central to our mission accomplishment. Therefore, it is our goal to continuously strive to maintain a high-performing, skilled IT workforce through enrichment opportunities, leadership development and a culture that promotes the sharing of intellectual capital.

Our ability to recruit, retain and re-train a skilled IT workforce continues to be a challenge confronting not only the Department of Transportation, but the Federal government in general. DOT is addressing the challenge of maintaining an agile workforce that is easily adaptable and highly skilled in mission critical competencies through its Strategic Management of Human Capital organizational excellence activities.

### **Goal**

Provide a world-class IT workforce for DOT.

### **Outcomes**

1. DOT as a top place to work for qualified and certified IT professionals.
2. A diverse workforce that is more closely aligned with current US demographics.
3. Increased job satisfaction.

### **Strategies**

1. Conduct labor market analysis to help understand work supply and demand, current and projected data.
2. Establish core competencies and standards.
3. Close targeted gaps in IT workforce.
4. Leverage existing workforce tools (e.g., eLMS, recruitment/retention bonuses, in-house/Federal-wide surveys) to ensure a high retention of critical employees.
5. Foster a diverse IT workforce by recruiting minorities, including those at Historically Black Colleges and Women's Colleges.

6. Expand retention strategies and succession strategies.
7. Improve the success of search processes in identifying underrepresented groups.
8. Participate in IT exchange program.
9. Invest percentage of budget for professional development and training.
10. Hold executives and departmental chiefs accountable for providing training (career development plans).
11. Increase Departmental agility by cross-training employees to encourage retention of institutional knowledge and sustaining best practices.

### Performance Indicators

*Table 5: Performance Indicators for Workforce*

Outcome	Performance Indicator
DOT as a top place to work for qualified and certified IT professionals	Percent of offers that are accepted.
Diverse workforce	Percent of DOT diversity targets achieved. Number of participants in OPM's IT Exchange Program.
Increased job satisfaction	Improved IT survey ranking (OPM) over previous year.

## **External Factors**

DOT workforce departures are the primary external factor that could affect our ability to achieve our IT workforce goal. Anticipated retirements and the move to a new headquarters building may have a significant impact within the IT community management levels during the next few years. The pending retirements will affect institutional knowledge and intellectual property. Moreover, the current workforce may require retraining to close the skills gap to function successfully in a future environment with advanced management tools, new hardware and software platforms, and networking capabilities. Aggressive marketing, outreach and recruitment initiatives will be necessary to attract highly skilled and diverse candidates to fill the next generation of DOT IT employees and managers.



## **APPENDIX 1: Management Challenges**

An unprecedented management challenge for the Office of the Chief Information Officer in fiscal year 2007 is the move to a new building. The Department of Transportation is relocating and consolidating approximately 5,800 of its employees to a new headquarters facility. This move is a major infrastructure component implementation: voice communication, data communications, data storage and engineering support. In order for the move to be successful, the Office of the Chief Information Officer will need the agreement of each operating administration to exhibit tolerance, understanding and appreciation of the significance of moving 6,000 computer desktops, 827 computing support servers, 413 business applications and 20,000 telephone extensions, all in just 11 weeks. The OCIO anticipates that most of the initiatives contained in this document will receive little or no attention during the move period, slated for April 2007.

While other challenges facing the OCIO in fiscal year 2007 are minor in comparison to the new building move, they merit formal citation.

### **GOVERNANCE**

For the first time, the OCIO has made a major paradigm shift in its governance process. The Chief Information Officer has required accountability from the modal CIOs through the process of voting on those issues that are cross cutting. The voting process is still in its infancy because the Office struggles to move forward while attempting to put into place processes simultaneously. The coming years will be the beneficiaries of the change.

The DOT Office of the Chief Information Officer owns the DOT IRM Strategic Plan and is responsible for implementing it, including the Governance provisions. This presents a management challenge to OCIO, because some DOT-level IT decisions are made by individuals, boards, and organizations that are not within OCIO's IT Governance structure.

The Governance outcomes in the DOT IRM Strategic Plan can be achieved only if improved Governance results in better decisions and those decisions are implemented. If those decisions are to be implemented at the DOT level, OCIO has to have the funding to be able to do so.

It bears mentioning that the IT oversight of the FAA will continue to require time and effort from the OCIO, especially for air traffic control modernization projects, which account for over 80 percent of the Department's IT budget. While some language has been offered to address the oversight authority of the OCIO, consensus has not been met.

## **SYSTEMS SECURITY AND PRIVACY**

The integrity, confidentiality and availability of information are the basis of maintaining the trust and confidence necessary for successful e-Government and Line of Business efforts. There are significant challenges to meeting these security and privacy objectives with growing needs for remote access and other factors, including:

- 1) Emerging technologies that do not have effective security;
- 2) Worldwide networks that provide access anytime from anywhere; and
- 3) A new generation of highly-skilled cyber-criminals.

The Department must address the following management challenges:

- Enhance Critical Infrastructure Protection.
- Enhance computer security reviews.
- Enhance the security protection associated with the HQ move.
- Enhance system contingency planning and testing.

## **ENTERPRISE ARCHITECTURE**

DOT must create customer centric services by working closely with its lines of business. To successfully achieve this DOT must address the following management challenges:

- Optimize the Enterprise
- Use Standard Technologies
- Create customer-focused services
- Ensure business continuity, and
- Governance.

EA is a critical element of every major IT system's business case (Exhibit 300), and should be a critical element of every IT initiative – major or otherwise. Other than OMB's requirement, on the surface, EA appears to be a sound way of approaching the management of organizations and their ability to respond to changing environments and requirements.

## **APPENDIX 2: List of Acronyms**

<b>CCA</b>	Clinger-Cohen Act of 1996
<b>CIO</b>	Chief Information Officer
<b>COE</b>	Common Operating Environment
<b>DOT</b>	Department of Transportation
<b>EIT</b>	Electronic and Information Technology
<b>eLMS</b>	Electronic Learning Management System
<b>FISMA</b>	Federal Information Security Management Act of 2002
<b>GPRA</b>	Government Performance Results Act of 1993
<b>IT</b>	Information Technology
<b>IRB</b>	Investment Review Board
<b>IRM</b>	Information Resource Management
<b>OA</b>	Operating Administration
<b>OCIO</b>	Office of the Chief Information Officer
<b>OMB</b>	Office of Management and Budget
<b>OPM</b>	Office of Personnel Management
<b>PMA</b>	President's Management Agenda
<b>PMP</b>	Project Management Plan