



FBI Information Technology Strategic Plan Synopsis

Preface

The following is a synopsis of the FBI's first Information Strategic Plan. That document is titled: Federal Bureau of Investigation Strategic Information Technology Plan FY 2005-2010. The plan was published in November, 2004, and was meant to be a baseline that would allow for future annual refinements and elaborations. A brief summary of that document follows.

Introduction

In the FBI Strategic Plan 2004 – 2009, the Director listed ten priorities for the FBI. One of those priorities was “to upgrade technology to successfully perform the FBI’s mission”. Information Technology (IT) was identified as a key enabling function. The purpose of this document is to present the FBI’s Plan for achieving that goal. We have identified that goal as an end-state to be realized by the year 2010. To accomplish that goal, the FBI needs a two-pronged overarching IT strategy and solution called *IT Vision 2010*:

- Provide and share “information on-demand anytime, anywhere for any mission reliably and securely” by aligning IT support to the Business/Mission with a pro-active Information Technology Vision.
- Institutionalize world-class IT Life Cycle Management processes, best practices, strategic IT insertion and measurement, and benchmarking techniques commensurate with leading organizations in the world

This Plan can best be presented by addressing five challenges and using them as a framework to detail the current, “As-Is”, transitional, and future “To-Be” states. The following five areas constitute the on-going challenges for the existing baseline FBI IT environment:

Challenge # 1: Information Sharing among historically Stove-Piped IT Systems

Challenge # 2: Better IT Alignment with Business Process Outcomes

Challenge # 3: Enterprise IT Framework and Process development

Challenge # 4: Robust IT Infrastructure which assures Continuity of Operations (COOP) and access to information in case of disaster

Challenge # 5: Information Assurance Balancing Security and Convenience



**Part I: Baseline or “As Is” Environment (2004):
Enterprise IT Foundational Processes Underway –
Mainly Stove-Piped Environment**

The Existing IT Environment - The current IT environment (circa FY 2004) has been designated as the baseline or “as-is” IT environment. This IT environment consists of:

IT Budget/Investment	CIO manages about 40-45%
IT Projects/ Programs	CIO manages about 24%
IT systems	CIO manages about 24%
IT Government personnel plus additional IT Contractors	CIO manages about 33%

The FBI Enterprise - The IT environment supports an overall FBI budget of approximately \$5 billion and supports approximately 30,000

personnel in 750 FBI locations world-wide, including Joint Terrorism Task Force (JTTF) members from other agencies with additional interfaces to the law enforcement and intelligence communities.

The IT infrastructure supports this hierarchical organization with a four-tiered architecture:

- Tier 1: Two main Enterprise Data Centers
- Tier 2: Ten Concentration Field Offices (CFOs),
- Tier 3: 46 Field Offices
- Tier 4: ~ 750 Resident Agencies, Off-Sites, Covert Sites, and Legats

Information resides in many internal separate databases in three separate security enclaves: Sensitive But Unclassified (SBU), Secret (S), and Top Secret/Special Compartmented Information (TS/SCI). The FBI maintains external information sharing connectivity with the Law Enforcement and Intelligence Communities through well-established networks at the three classification levels. The six main IT systems/networks that facilitate internal and external information access and sharing are:

Enclave	Internal Network	External Network
TS/SCI	SCION	JWICS
S	FBINET	SIPRNET
SBU	SBUNET	LEO/CJIS WAN

Assessment of IT Environment: Challenges The challenges in achieving world-class IT status to meet ever-changing FBI mission needs are five-fold:



- **Challenge #1: Information Sharing among historically Stove-Piped IT Systems**
 - Exigent tactical mission needs in each functional area have led to sub-optimized, stove-piped IT solutions over time in three enclaves
 - A lack of standard interfaces between applications, databases, and little use of industry standard protocols has limited system inter-operability and collaboration
 - Inability to query across stovepipe database systems prevents federating a query across FBI databases and receiving an integrated response
 - Inability to exchange real-time digital information limits collaboration in the intelligence community
- **Challenge #2: Better IT Alignment with Business Process Outcomes**
 - Enterprise mission/business requirements and business architecture under development
 - Enterprise business performance goals/outcomes under development
 - Mission changes (e.g., Intelligence) occur before business architecture changes which precede outcome changes
 - Applications development requires more direct user involvement
 - Enterprise case management system is limited by inability to automatically and efficiently extract metadata and post documents and exhibits
- **Challenge #3: Enterprise IT Framework and Process development**
 - The IT budget and Information Technology Investment Management (ITIM) process is not centrally controlled or managed by the Chief Information Officer (CIO)
 - No Enterprise IT Life Cycle Management Process or measurement in-place
 - No Enterprise Architecture (EA) exists with technical standards, metadata, and interoperability criteria
 - Outdated system engineering, acquisition, operation, and maintenance practices
- **Challenge #4: Robust IT Infrastructure which assures COOP and access to information in case of disaster**
 - IT infrastructure foundation is not commensurate with industry standards
 - In case of major disasters, major failures, or commercial service interruption, there is limited ability to restore services or to access corporate data/information
 - Core set of mission critical information and systems is not well defined
- **Challenge #5: Information Assurance Balancing Security and Convenience**
 - Role-based access controls for information across and within classifications levels is lacking
 - Plans to counteract insider and external threats while providing information access under development
 - Need to prevent unauthorized manipulation of evidence admissible in court limits ability to store documents and images in a secure digital fashion



- Special releasability restrictions on highly sensitive information or due to specific legal or legislative considerations creates information management complexity within each of the three enclaves

Interim Accomplishments The FBI has countered these challenges with some impressive interim IT accomplishments to prepare the FBI to adapt to changing missions. A sampling of some key events to address these challenges is highlighted below:

- **Challenge #1:** Information Sharing among historically Stove-Piped IT Systems
 - Information Sharing Initiative established with law enforcement community (e.g., MISI, N-DEX, LEO) with additional participation in Law Enforcement Information Sharing Program (LEISP) development.
 - Classified connectivity established into databases through the Secret Internet Protocol Network (SIPRNET), Joint Worldwide Intelligence Communication Service (JWICS) and Defense Message System (DMS) for Counter Terrorism and Intelligence needs.
- **Challenge #2:** Better IT Alignment with Business Process Outcomes
 - Baseline FBI Strategic Plan Published with Business Goals, Objectives and Performance measures. Strategic IT Plan aligned with Strategic Plan
 - Intelligence immediate/near-term IT requirements vetted and published
 - Mission owners participation in all IT boards to ensure business drives enterprise architecture and IT portfolio
- **Challenge #3:** Enterprise IT Framework and Process development
 - Enterprise IT governance processes established with LCMD (Life Cycle Management Directive) published (9 life cycle phases, 7 control gates, 14 key support processes)
 - Enterprise IT governance boards established to coincide with LCMD including an additional IT Advisory Board comprised of Assistant Directors from all Divisions (Mission Owners)
 - Baseline enterprise architecture published with emphasis on business architecture
 - Enterprise Office of the CIO (OCIO) IT Metrics Report published monthly using Balanced Scorecard methodology
 - Enterprise IT Policies (65) being published
 - Enterprise tool selected for Enterprise IT Portfolio, IT Project/Program Management and IT Investment Management
 - Master List of IT Programs/Projects and Master List of IT Systems established to begin the consolidation process
 - Commitment to industry and government benchmarks (e.g., Software Engineering Institute) SEI Capability Maturity Model Integrated (CMMI) Level 3; Government Accountability Office (GAO) EA Management Maturity Framework (MMF) Level 5
- **Challenge #4:** Robust IT Infrastructure which assures COOP and access to information in case of disaster
 - Aging enterprise classified network and computing infrastructure upgraded to industry standards under Trilogy Program



- Network and computing redundancy introduced throughout the enterprise at Tiers 1, 2 and 3 through Trilogy
- COOP Tool selected (also used by IC) and certification training established for select CIO staff.
- **Challenge #5: Information Assurance Balancing Security and Convenience**
 - Comprehensive Enterprise Information Assurance Program implemented to counteract insider and external threats with a defense-in-depth approach

These interim accomplishments represent a commitment by the FBI to address the challenges from a tactical and strategic perspective, while ensuring enterprise business requirements and outcomes drive the Enterprise Architecture. While these challenges will take time to address, the FBI intends to benchmark itself against known Industry and Government standards (CMMI and GAO MMF) to establish a world-class IT status by 2010 in an incremental approach.



Part II: PMA/DOJ/FBI Roadmap and CIO Framework (Transition Plan: How We Get There)

FBI Information Technology Strategy - Our strategy during the five year planning period combines enterprise-wide governance and technical initiatives with specific projects and initiatives that support particular strategic objectives and performance goals that contribute to achieving the missions of the FBI. The overwhelming majority of FBI IT expenditures are managed by FBI HQ divisions on behalf of the total FBI population, which is distributed across the country and increasingly around the world. Similarly, the missions of the FBI tend to align with particular FBI HQ divisions although there is substantial overlap across divisions and of course all missions are addressed by every field office. Accordingly, a substantial portion of this strategy involves effectively coordinating the IT efforts of the FBI HQ divisions.

In the continuing effort to improve the strategic planning process and make that process relevant to all aspects of the FBI’s operations, the Deputy Director’s office is developing a program known as Comprehensive Operational Management Plan Advancing Specific Strategies (COMPASS). This will be a web based application that provides information on specific goals, objectives, and performance outcomes for each division, both, headquarters and field, in the form of targeted actions. Specific progress on those objectives will be collected by the system and be available to senior management at any time on-line. As COMPASS is developed, it will become useful to the IT strategic planning process to aid in the measurement of specific strategic outcomes. This will allow us to better trace the effects of specific IT systems on the strategic outcomes and aid in our ability to measure them.

Understanding of FBI’s Strategic Mission/Business Needs Table 1 below summarizes the goals and objectives by subject area. All of these elements must be addressed by an enterprise IT strategy.

Table 1. Summary of FBI Strategic Plan

FBI Strategic Plan Summary	
FBI Mission	To protect and defend the United States against terrorism and foreign intelligence threats, to uphold and enforce the criminal laws of the Unites States and to provide leadership and criminal justice services to federal, state, municipal and international agencies and partners.
Core Values of the FBI	Adherence to the rule of law and rights conferred to all under the Constitution; Integrity through everyday ethical behavior; Accountability by accepting responsibility for actions and decisions, and their consequences; Fairness in dealing with people; and Leadership through example, both at work and in our communities



Table 1. Summary of FBI Strategic Plan (continued)

Strategic Goals: Achieving The Mission	
Intelligence	Establish an enterprise-wide intelligence capability that optimally positions the FBI to meet current and emerging national security and criminal threats.
Counterterrorism	Protect the United States from terrorist attack.
Counterintelligence	Protect the United States against foreign intelligence operations and espionage.
Cyber	Protect the United States against cyber-based attacks and high technology crimes.
Public Corruption	Reduce the level of public corruption that has an impact in the United States.
Civil Rights	Prevent the violation of federal civil rights as guaranteed by the United States Constitution.
Transnational/National Criminal Enterprises	Reduce the impact transnational/national criminal enterprises have on the United States.
White Collar Crime	Reduce the level of significant white collar crime.
Significant Violent Crime	Reduce the level of significant violent crime.
Support to Other Agencies	Increase FBI support to our federal, state, county, municipal, and international partners.
Strategic Goals: Human Capital	
Human Capital	Establish a human capital capability that ensures the FBI maintains a preeminent work force at all times.
Strategic Goals: Tools	
Security	Establish an enterprise-wide Security Program that protects our people, information, and capabilities.
Information Technology	Establish a secure, flexible, and modern information technology (IT) system that supports the collection, analysis, processing, and dissemination of information.
Investigative Technology	Effectively utilize applied science and engineering resources to empower the FBI's investigative and intelligence operations and the thwart the techniques of our adversaries.
Criminal Justice Information Services Division	Improve CJIS Division's ability to provide timely and relevant criminal justice services to the FBI and to authorized law enforcement, criminal justice, civilian, academic, employment, and licensing agencies.
Forensics	Establish a world-wide network of scientific services that maximizes forensics in combating terrorism, cyber-based attacks, and crime.
Records Management	Establish a state-of-the-art record keeping system.

PMA/DOJ/FBI Roadmap and CIO Framework- A comprehensive framework has been adopted from the Chief Information Officers Council to establish a roadmap for meeting the President's Management Agenda (PMA), Department of Justice (DoJ) and FBI Strategic and Human Capital Plans. The CIOs Council has designated 11 competencies required of Federal CIOs. They are depicted in Figure 1 to the right.



Figure 1. Eleven CIO Competencies



The eleven CIO Competencies are used to integrate the FBI Strategic Plan with the FBI Human Capital Plan and separate division and program plans. The FBI Strategic Plan clearly describes the ongoing transformation of the FBI to meet our expanded mission. It forecasts the environment we will face in each of our major program areas (mission and support). The FBI Human Capital Plan describes how the FBI will establish a preeminent workforce at all times. In concert with the transformation envisioned in these two FBI plans, the FBI IT Plan addresses how information technology enables and supports FBI transformation while ensuring alignment with the President’s Management Agenda, Department of Justice and FBI strategic goals. This plan provides specific applications and systems for each area/objectives that are: (1) existing, (2) under development, and/or (3) planned. It then shows how these applications and systems support specific strategic objectives and performance goals from the FBI Strategic Plan and Human Capital Plan. The plan is structured to show how the FBI will achieve this vision incrementally over time beginning in 2004, transitioning over 5 years and culminating in the goal vision (2010). A “framework or roadmap” of how this plan aligns with the President’s, Departments and Agency Goals is illustrated in Figure 2 below.

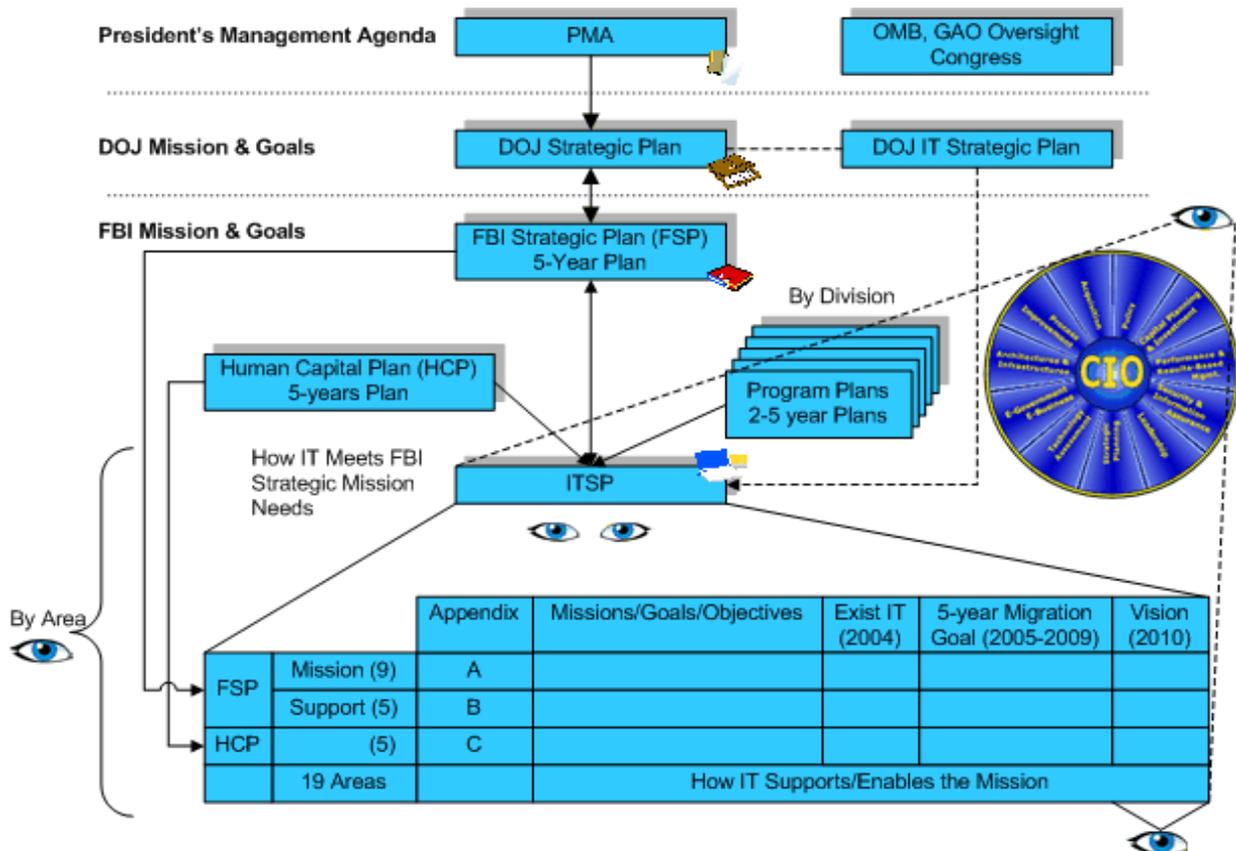


Figure 2. Roadmap for meeting the President’s Management Agenda, Department of Justice (DOJ) and FBI Strategic and Human Capital Plan

Enterprise IT Framework - The upgrade and modernization of FBI Information Technology, in order to successfully perform the FBI’s missions, has been identified as a top 10 FBI priority. Key management actions, consistent with this high priority, have been taken. An



IT management process to maximize the value of IT acquisitions and to assess and manage risks has been adopted. This process is depicted Figure 3. IT management processes have been integrated with the processes for budgeting, financial management, and making program management decisions. Information security policies, practices and procedures have been developed and are being followed to protect FBI information technology resources.

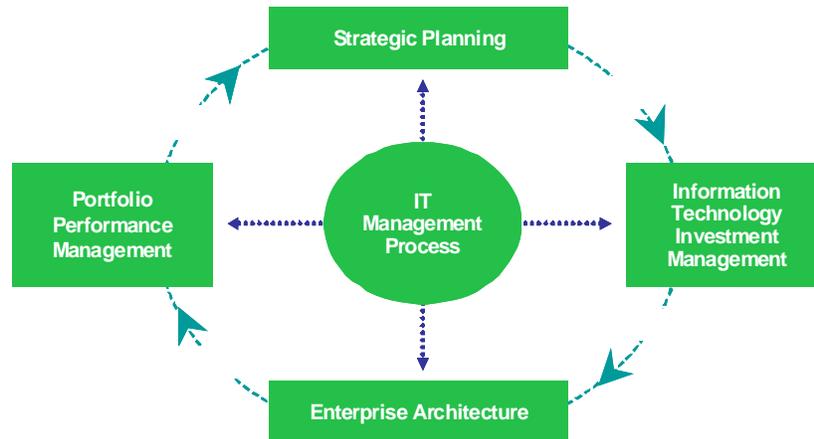


Figure 3. Guiding IT Disciplines

The guiding disciplines underlying the governance of FBI Information Technology activities in addition to Strategic Planning include:

Portfolio Management

In FY 2003, a portfolio management project was initiated to evaluate the FBI’s legacy IT portfolio in response to various oversight requirements, in particular, the GAO’s Audit of the FBI’s management of IT. The portfolio management initiative will develop and maintain an enterprise-wide portfolio of IT assets. A key activity of the portfolio management project is analyzing the functional alignment of assets to mission coupled with the technical performance. The combined analysis of the assets will determine which investments may be leveraged or exploited; replaced or outsourced; or retired. The outcome of this effort will result in a powerful decision making tool in the IT investment process which potentially can redirect resources (both fiscal and personnel) towards the FBI’s most critical requirements.

Information Technology Investment Management (ITIM)

The FBI has adopted a classic *ITIM Program*. ITIM is integrated into the budget and strategic planning process. The ITIM program follows the “GAO Framework for Assessing and Improving Process Maturity” and complies with all of the associated Congressional and Federal mandates. In particular, documents responsive to Office of Management and Budget (OMB) Circulars, which are utilized within the ITIM Program include: OMB Exhibit 300 “Capital Asset Plan and Business Case” and OMB Exhibit 53: An agency’s “IT Portfolio.”

Enterprise Architecture



An aggressive effort is underway to complete the initial FBI Enterprise Architecture (EA) during fiscal 2004. The FBI's EA is comprised of a baseline (sometimes called the "as is") architecture, a target (sometimes called the "to be") architecture, and a transition plan and sequencing plan for the migration from the current baseline to the future target. The EA (Figure 4) consists of the following four sub-architectures: Mission/Business, Application, Data/Information, and Technology. An interim EA will define the architecture for two years into the future to establish funding requirements for defined projects that must be implemented each year to move toward the target architecture.

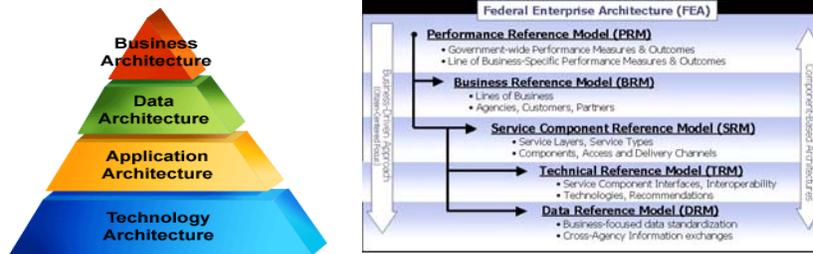


Figure 4. Enterprise Architecture Structure

Figure 5 displays how the Plan will integrate business objectives with the different levels that the enterprise architecture must address.

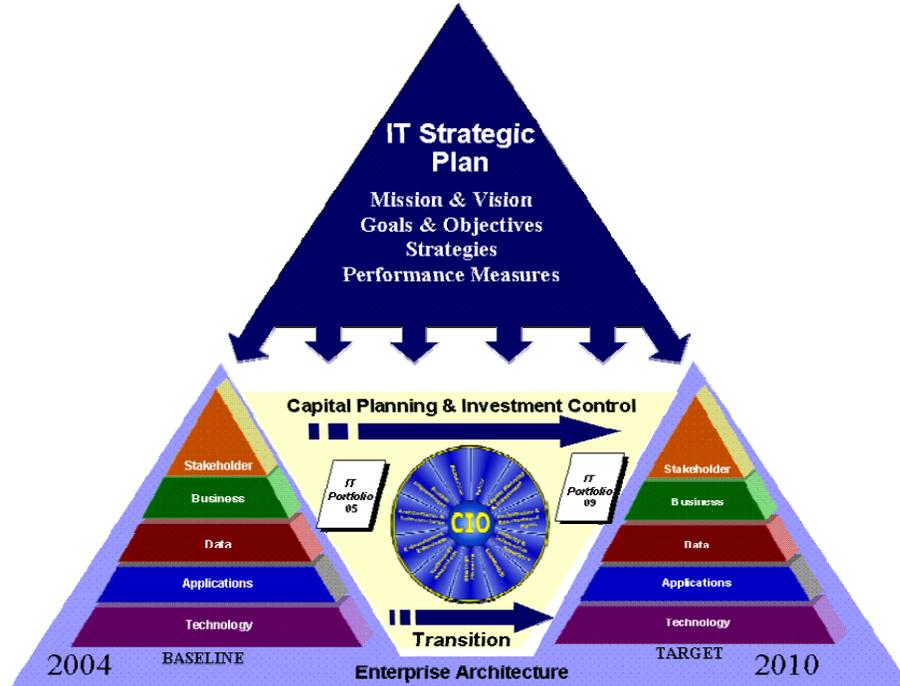


Figure 5. (U) Integration of IT Strategic Plan into ITEM and EA

Technical Initiatives



During the five year planning period, the FBI will pursue several enterprise-wide technical initiatives. These enterprise initiatives are directed to increased effectiveness and toward reduced total costs of ownership.

Mission effectiveness technical initiatives during this period include:

- Ubiquitous access to FBI secure and non-secure voice, data, video teleconferencing, and information systems
- Web-enabled applications
- Work group collaboration
- Enterprise ownership, control and (logical) centralization of information is the policy of the FBI and FBI IT systems will enforce this policy.
- Migration from separate TS/SCI, Secret, SBU and Unclassified enclaves to multiple secure layers from a common desktop
- As voice recognition and optical character recognition technologies become more robust and reliable, the FBI will broadly adopt these technologies to improve productivity
- Single sign-on, Public Key Infrastructure (PKI) and digital signature technology will be introduced to both multiply mission effectiveness and to increase security.

Total cost of ownership reduction initiatives during this period include:

- Purchase of common desktop, server and peripheral hardware, and software from standard product lists (SPL).
- Migration from the high touch desktop support environment of today to no-touch support tomorrow.
- Migration from support staff dispatched to the worksite to effect service restoration of failed desktop systems to an end user direct exchange model.
- Ability of employees to perform their work from any comparable desktop will allow employees to remain near fully productive even when their dedicated equipment has failed.
- Our data centers will achieve near “lights out” operational capability where systems and database administration staffs need not be co-located with the equipment.
- Analysis of telecommunications circuit and service utilization, elimination of inactive assets, adjustment in committed information rates to improve return on the recurring investment.



Part III: IT Vision 2010: Target IT Environment ("To Be")

IT Vision 2010: "World-Class" IT Addresses Five Challenges in an Enterprise Framework - The key elements that comprise the FBI IT Vision 2010 include fully addressing the five-fold challenges facing the FBI in a global environment. This has been summarized in a Table 2 below:

Table 2. IT Challenges and Solutions

Challenges	Proposed Fix by 2010	Benefits
1. Information Sharing among historically Stove-Piped IT Systems	Integrated Enterprise IT Systems within ICSIS-compliant EA promote information sharing within and between 3 enclaves with "tear-line" data	Seamless Information Sharing with Law Enforcement and Intelligence Community with appropriate Role-Based Access is the norm, not the exception
2. Better IT Alignment with Business Process Outcomes	GAO MMF Level 5 EA updated Annually has on-line Performance Reference Model, Business reference Model clearly established so that Services, Technical and Data Architecture achieves business outcomes and is measurable	Clear alignment of technical architecture to achieve business outcomes can be measured through Mission metrics and IT metrics. Intelligence, Counter-Terrorism and Counter-Intelligence are key FBI success story by 2010
3. Enterprise IT Framework and Process development	IT Governance Process (LCMD, Boards, Policies etc.) has matured to CMMI Level 3 with control of all IT Portfolio of 20-30 IT Projects/Programs; Clearly established IT Product/Service Offerings; and EA-compliant systems	CIO-controlled Enterprise IT Budget, Process and Framework facilitate better IT investment management to achieve Mission/Business outcomes
4. Robust IT Infrastructure which assures continuity of operations (COOP) and access to Information in case of disaster	IT Infrastructure has exceeded Industry standards by conforming to IC-caliber capability in Networking & Computing Capacity Performance for Imagery. COOP and COG facilitated at the Enterprise Level with load-balanced (fail safe) access to mission-critical information and consistent with IC. Central Records Complex (CRC) is being established for central records and Enterprise COOP	Enterprise Portal with standardized tool suites provides user with ability to have integrated access to information in an easy-to-use manner with quick response, reliable performance and security=y on 24x7x365 days/year basis
5. Information Assurance Balancing Security and Convenience	Data Classification requirements and metadata tagging facilitate data security levels under the EA (LCMD). Information Assurance/IT Policies facilitate role-based access to information (as identified by Mission Owners). The norm is sharing except for sensitive special access programs or other caveats. Strategic IA Technology Infusion leveraged to implement policy	The appropriate and accurate classification of data/information and definition of roles of individuals (internal and external) with access to data/information provides the correct balance between security and convenience



Enterprise Architecture 2010: Single Enterprise Easy-to-Use Portal, Standardized Tool Suite, Role-Based Access to All Information in any Enclave - In FY05, the FBI began creating a prototype enterprise technical architecture, which will be the basis for evolution into the “To-Be” vision. Simply put, the enterprise technical architecture will typically have five major components: (1) An enterprise portal that serves as a gateway to all the information and tools of the FBI, (2) Middleware that contains enterprise applications and business logic, (3) Services that unlock the information stored in legacy databases and new enterprise data/information warehouses, (4) An underlying networking and computing infrastructure, and (5) An Enterprise system and security management infrastructure to oversee quality of services being provided to the user, while ensuring adequate information assurance.

Enterprise Architecture 2010: Common, Standardized, Enterprise IT Applications and Products/Services Suite through An Enterprise Portal - Enabled by the common infrastructure, and in turn providing IT support to all the missions and most of the goals and objectives of the FBI are a number of Enterprise wide IT applications and Products/Services. EA 2010 is comprised of a standardized suite (>80%) of common capabilities and support services, which are essential underpinnings that enable us to communicate, collaborate and share information seamlessly in 2010. Mission-unique services (<20%) shall be available in cases where needs are more localized or too-specific, thereby obviating need for an enterprise solution. These standardized product and service offerings will be published by the CIO and maintained under strict configuration control. This facilitates a service supply chain with known controls to guarantee service levels to the customer/user.

The Portal will serve as a single access point for all administrative, programmatic, acquisition and mission Applications, data and products/services. The Investigative Data Warehouse (IDW) will allow queries across unstructured and structured data and enable access to legacy data sources and to new data sources from within and outside the FBI.

Enterprise Architecture 2010: Common, Standardized, Highly Redundant IT Infrastructure with 99.99% Availability and COOP - The EA shall provide guaranteed levels of performance with Service Level Agreements (SLAs) for all services and infrastructure. enterprise COOP shall be maintained 24x7x365 days/year for mission critical data/information in a fail-safe (load-balanced) manner at 2-3 locations so that information will be available in the event of a disaster.

In addition, in order to achieve robust security across three security enclaves, the enterprise technical architecture will provide confidentiality, integrity and authentication services. PKI is being implemented FBI-wide to provide strong authentication and ensure non-repudiation and Discretionary Access Controls (DAC) are provided to protect confidentiality based on records and even data fields. Protect Level (PL) 3 security will allow fine grain access control, marking/labeling data transmitted or stored to reflect the sensitivity of the information, and capturing enhanced audit information. This common applications and services suite enables the FBI to support particular goals and objectives within business/mission needs as defined by the mission owners.

Table 3 below shows how both the eleven FBI Key Elements and four FBI Challenges link to the four DOJ IT Goals from the DOJ IT Strategic Plan. The FBI IT Strategic Plan’s transition



plan is built around and will be expanded to fully address these elements and overcome the challenges. FBI IT Vision 2010 will provide an “end-state” that delivers this functionality to agents, analysts and support personnel.

Table 3. DOJ/FBI Driver Cross-Reference

DOJ IT GOALS	FBI KEY ELEMENTS	FBI CHALLENGES
1.Share Information Quickly, Easily, & Appropriately – Inside & Outside of DOJ	3. Readily Accessible Information 4. External Investigators provided access to information 5. Information Sharing & Collaboration the rule, not the exception 6. Rapid Collaboration across Govt.	1. Information Sharing among historically Stovepiped IT systems
2.Secure & Protect Information	1. Anywhere, Anytime, Any Task 2. Community of Interest Separation 7. Electronic Records, Electronic Signature, No Sneakernet	5. Information Assurance Balancing Security & Convenience
3.Provide Reliable, Trusted & Cost-Effective IT Services	8. Fast, Reliable, Invisible IT Infrastructure 9. Common Services & Technology Across the Enterprise 10.Common Look and Feel to all Enterprise Services 11.”No Touch” Platinum Support for Everyone	2. Better IT Alignment with Business Process Outcomes 4. Robust IT Infrastructure which assures continuity of operations (COOP) & access to Information in case of disaster
4.Use IT to Improve Program Effectiveness & Performance	Human Capital Plan	3. Enterprise IT Framework & Process Development