United States Department of Justice

Federal Bureau of Investigation

Information Technology Strategic Plan
FY 2010 – 2015

CIO's Vision

"…to deliver reliable and effective technology solutions needed to fulfill the FBI's mission anytime, anywhere, on time and on budget…"

Chad Fulgham, Chief Information Officer

Chief Information Officer's Message

This IT Strategic Plan is focused on using IT as the enabler to collect, store, transport, display, analyze and disseminate information in support of the FBI's lines of business. Our customers, the agents and analysts in the field and headquarters, expect us to deliver timely, reliable and effective IT solutions, providing accurate and actionable information to those carrying out the FBI's mission. I envision a vastly improved and agile IT environment that will better serve an increasingly proactive FBI enterprise. With an enterprise perspective for improving strategic processes, tactical activities and logistical technologies, we will achieve increasing benefits to the mission owners, measured by desired outcomes. Through careful planning and cooperation with our many users and stakeholders we will meet our IT strategic goals outlined in this plan.

Executive Summary

The FBI has a dual mission to enforce federal laws and protect the national security. In fulfilling its mission, the FBI continues to fuse the requirements of the domestic and foreign Intelligence and Law Enforcement Communities to meet the changing national security threats. In parallel, the FBI's Information Technology (IT) capabilities are evolving in order to improve operational effectiveness and enhance organizational flexibility. Modernization and enhancements to the IT infrastructure are necessary to support FBI priorities and fulfill Department of Justice (DOJ), Office of the Director of National Intelligence (ODNI), Office of Management and Budget (OMB) and other external mandates and requirements.

FBI Priorities

- Protect the United States from terrorist attack
- Protect the United States against foreign intelligence operations and espionage
- Protect the United States against cyber-based attacks and high-technology crimes
- Combat public corruption at all levels
- Protect civil rights
- Combat transnational / national criminal organizations and enterprises
- Combat major white-collar crime
- Combat significant violent crime
- Support federal, state, local and international partners
- Upgrade technology to successfully perform the FBI's mission

The FBI requires transformation to the next generation of IT infrastructure, where emerging technologies provide a more resilient and agile environment. The Next Generation Network (NGN) project will upgrade the FBI's Wide Area Network (WAN) from its current Asynchronous Transfer Mode/Frame Relay (ATM/FR) point-to-point Permanent Virtual Circuit (PVC) based architecture to one based on Internet Protocol (IP) Multi Protocol Level Switching (MPLS). NGN will modernize the FBI's network infrastructure, aligning it with current industry best practices. NGN will consolidate the four-tiered Trilogy network design into a common IP based core network capable of supporting integrated IP data, IP voice, IP video services, and other future applications.

The Next Generation Workspace (NGW) project will transform the FBI through deployment of the best-of-breed workspace technology. NGW will equip FBI users with new and efficient ways to communicate and collaborate with their fellow employees across the globe. The FBI also recognizes the need to align system development and data repositories across all mission areas, rather than incentivizing the development of stove-piped technologies, as it is currently. This transition will enable the migration to a true shared services environment that will further improve the effectiveness and efficiency of the FBI and the Intelligence and Law Enforcement communities.

The FBI continuously evaluates ways to improve operational efficiencies and conserve valuable resources by combining similar services and facilities. The identification and elimination of duplicative systems, applications, databases and networks will free up resources to be applied to new and enhanced IT capabilities. Along with our Law Enforcement and Intelligence Community partners, the FBI recognizes that community-wide sharing capabilities require an in-depth understanding and harmonization of the underlining data. This in turn requires the agreement upon and implementation of standards and governance across the communities.

In conjunction with improving information sharing capabilities, the FBI recognizes the need to develop and implement a comprehensive Knowledge Management (KM) strategy. The KM strategy will promote a culture of data and information sharing within the FBI that will enable the development of knowledge. The FBI will expand its focus on customer service and satisfying the needs of both mission and support area end-users of IT. Proactive end-user support and enterprise solutions development will be top priorities. The FBI will initiate IT activities in accordance with this plan, supported by an integrated FBI Enterprise Architecture (EA) and IT Investment Management (ITIM) process.

Introduction

"We can't solve problems by using the same kind of thinking we used when we created them." - Albert Einstein

FBI Mission

Since its creation in 1908, the FBI's mission has been to investigate federal crimes and bring criminals to justice. After 9/11, it became necessary to enhance the FBI's intelligence program and broaden its role in the Intelligence Community. To reflect this shift in focus the FBI re-aligned its mission statement, which now reads:

"The mission of the FBI is to uphold the law through the investigation of violations of federal criminal law; to protect the United States from foreign intelligence and terrorist activities; to provide leadership and law enforcement assistance to federal, state, local and international agencies; and to perform these responsibilities in a manner that is responsive to the needs of the public and is faithful to the Constitution of the United States."

"…In today's global environment, information technology remains key to how the FBI conducts its business – capturing information that can be instantly retrieved and shared as we build our investigations, providing the means to collaborate across distances, and keeping our data secure…"

FBI Director Mueller
Appointment of FBI CIO Chad Fulgham
December 8, 2008

This mission rests between two communities led by cabinet-level departments requiring the FBI's extensive investigative and analytical expertise – the Law Enforcement Community (LE) under the Department of Justice (DOJ) and the Intelligence Community (IC) under the Director of National Intelligence (DNI). The national security and criminal threats faced by the FBI, from terrorism to national/international criminal activities, are becoming more complex and multi-dimensional. The global

nature of the threats requires the FBI to think and act with a diversity of mindset, unity of purpose and vigilance toward the future. Reliable, effective, efficient and responsive IT capabilities and services are necessary to support our mission, anywhere, anytime.

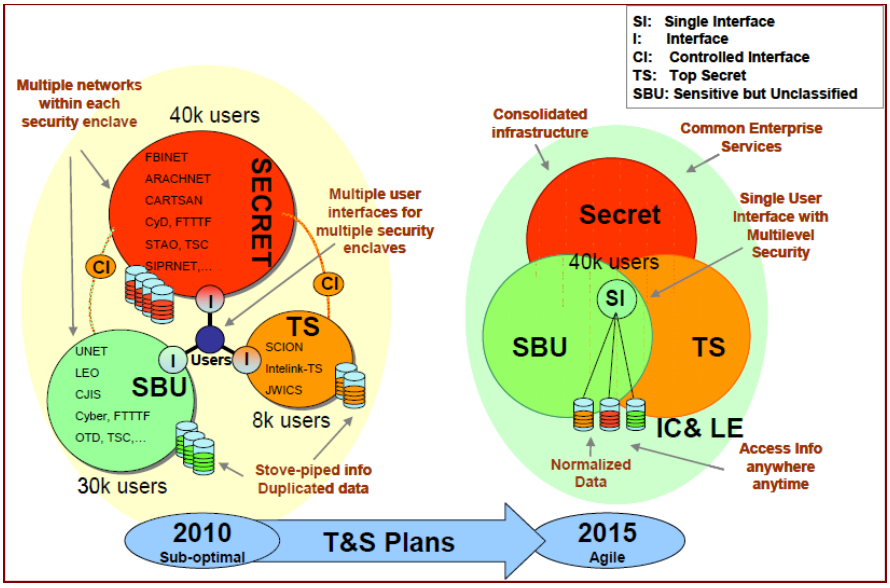
Scope

This FBI IT Strategic Plan (ITSP) was developed on the foundation of current legislation and directives, and maps to the DOJ Strategic Plan, DOJ ITSP and the FBI Strategy Management System (SMS). It aligns with the enterprise perspective for improving strategic processes, tactical activities and technology to achieve increasing benefits to the mission owners that can be measured in desired outcomes. The target audience for the ITSP includes FBI Senior Executives, mission owners, IT enterprise architects, IT program managers and financial planners.

Vision

All areas of the FBI mission — law enforcement, intelligence, counterintelligence, technology, human capital and management — require a resilient, agile and sustainable IT infrastructure with advanced technologies for the FBI to achieve its mission. This Strategic Plan lays the groundwork for enabling a portfolio of IT within a highly capable Enterprise Architecture (EA), ***delivering reliable and effective technology solutions needed to fulfill the FBI's mission anytime, anywhere, on time and on budget.***

The envisioned transition to an agile enterprise will emphasize on-demand access for real time, 24x7, information accessibility at its earliest point, with an enabled all-source, secure information sharing capability. To achieve this, the FBI will need a flexible and secure infrastructure, enabling integration of data through a supporting network structure as depicted. To administer the enterprise, the FBI requires enterprise-wide engineering and management of IT resources with common, standardized, shared IT services. These resources will be mission focused and mission driven, providing innovative IT solutions with cross-domain services to improve information-to-operations integration. The future-state will include common enterprise services, a single user interface with multi-level security and normalized data.



Guiding Principles

The FBI ITSP guiding principles are to clearly identify, document and promote the FBI's IT strategic direction; establish and leverage IT performance measures; and track aggregate progress toward achieving goals and objectives that guide strategic management of the FBI's information resources. These principles guide the mission of the FBI IT to:

- Use IT to enable the mission areas of the FBI to perform at their highest potential.

- Develop enterprise approach to integrate processes and technologies.
- Promote collaboration, partnerships and information sharing.
- Comply with necessary mandates.
- Provide outstanding customer service.

The FBI mission drives the SMS Goals and Objectives and this IT Strategic Plan. These guiding principles focus the strategic planning process.

Goals and Objectives

IT goals and objectives articulate the role of technology in support of the FBI's mission. The IT goals and objectives described in the following table address the key areas of focus and change needed to realize the IT vision outlined in the previous section.

Vision: ***Deliver reliable and effective technology solutions needed to fulfill the FBI's mission anytime, anywhere, on time and on budget.***	
Goals	**Objectives**
1.0 Create a Resilient, Agile and Secure Infrastructure	1.1 Provide a comprehensive, resilient and modernized technical infrastructure with "right sized" Data Center(s) and COOP capabilities.
	1.2 Enable user communication, collaboration and cross-domain information access through secure, enhanced and flexible networks.
	1.3 Provide enterprise users with standardized IT solutions and services using enhanced infrastructure support.
2.0 Improve Analysis, Collaboration and Information Sharing	2.1 Deploy Enterprise-wide Analytical capabilities.
	2.2 Advance Knowledge Management.
	2.3 Improve ability to provide timely and relevant information sharing with FBI LE and IC partners.
3.0 Transform Our IT Workforce	3.1 Become a center of excellence and employer of choice.
	3.2 Align workforce skills to achieve IT strategic goals and objectives.
	3.3 Promote continuous learning and formal training programs for proactive skills development.
4.0 Improve the overall Management of Information Technology	4.1 Provide enterprise solutions that support multiple mission areas.
	4.2 Leverage technology and science for innovative new solutions.
	4.3 Recommend IT solutions for enterprise services.
	4.4 Optimize the FBI portfolio of IT resources (assets, projects, investments) through effective governance processes.
5.0 Enhance Customer Satisfaction	5.1 Improve customer service, communication and coordination.
	5.2 Improve tracking, quality and timeliness of IT requests and customer service needs.
	5.3 Increase Enterprise IT marketing efforts.

Key Drivers

The FBI ITSP was developed through analysis of the external and internal environments and identification of the key drivers impacting the strategy for the FBI. The key drivers include the FBI's evolving mission and how that impacts IT requirements, identified strategic gaps, the strategy management system, integrity and compliance initiatives, legislative mandates, technology trends, workforce transformation and financial challenges.

IT as a Mission Enabler

Increasing mission complexity and demanding customer requirements require a forward-focused strategy, with stable execution of current operations. In its current IT enterprise, the FBI operates under a distributed and stove piped environment, supported by numerous servers running countless applications on multiple systems. The current "as-is" IT infrastructure has allowed the FBI to *meet* the essential needs of its users. However, increased levels of efficiency and standardization at multiple technology levels (i.e., networking, data, applications and infrastructure) are required to address our continually evolving and expanding mission requirements. FBI IT must change accordingly in order to meet these increasing demands.

Strategic Gaps 2011 - 2015

The Director's Budget Planning Guidance for 2011-2015 Memorandum to all FBI Executive Assistant Directors and Assistant Directors dated November 19, 2008 identified six IT mission gaps. These gaps correspond with the FBI's SMS Themes. The first gap is with surveillance technologies, where the need has arisen for enhanced staffing and sustaining systems. Another gap involves the rapid evolution of digital technologies, enabling the Intelligence Community to remain current with lawful intercept technologies and avoid the possibility of "going dark".

The IT infrastructure was also identified as a strategic gap. Specifically, the FBI needs to address data center relocation, Investigative Data Warehouse re-engineering, legacy mainframe applications replacement, information sharing capabilities, and network deficiencies. A strategic gap identified the need to enable SENTINEL case management capabilities for SCION and UNet. Additional strategic gaps identified the need for additional digital forensics capabilities to eliminate backlogs and ensure that growth in cheap media storage does not overwhelm the FBI's capabilities, and for FBI's biometrics to evolve the legacy identity systems to a multi-modal biometrics system.

Alignment to the Strategy Management System

Through the FBI's SMS, the Director identified the enterprise shifts and organizational strategy that guides the FBI's collective efforts. The FBI's SMS uses strategy articulation, performance measurement and a concise management communication 'language' to enable organizations to make proper decisions and manage toward the right solutions. Combined with the "Strategy Drives Budget" initiative, SMS provides a holistic view of an organization's overall performance by integrating financial measures with other key performance indicators around customer needs, internal business processes and learning and development tools.

FBI Office of Integrity and Compliance (OIC)

The FBI's OIC mission is to develop, implement and oversee a program that ensures processes and procedures are in place to promote compliance with the letter and spirit of applicable laws, regulations, rules and policies. IT capabilities and solutions are needed to enforce our policies and prevent instances of legal noncompliance.

Legislative Mandates and Directives

The ITSP's development and evolution respond to the legislative mandates in the Clinger-Cohen Act of 1996 (CCA) and in the Paperwork Reduction Act of 1995, which specify that agencies shall "develop and maintain a strategic information resources management plan that shall describe how information resources management activities help accomplish agencies' missions". Numerous existing Federal laws and regulations, such as the President's Management Agenda (PMA) and OMB and DOJ Directives, prescribe, influence and guide the development and execution of FBI IT policy, programs and projects. In addition, compliance with the CCA, the Government Performance and Results Act, the E-Government Act, the Federal Information Security Management Act of 2002 (FISMA) and Section 508 of the Rehabilitation Act, requires a strong emphasis on performance improvement, accountability for achieving results, security, accessibility and cost efficiency.

Technology Trends

IT advances at a rate that requires constant review and evaluation of new and emerging technologies. This becomes both an advantage and disadvantage to industry and government alike. Businesses look to emerging technologies for a competitive edge and are eager to adopt and converge the "leading edge" systems and software into their infrastructures. Unfortunately, emerging and advanced technologies and trends also lead to advanced criminal and intelligence/counter-intelligence activity concerns. To address these concerns, the FBI requires evaluation, analysis, adoption and integration of "selected" technologies and industry trends that advance the mission.

IT Workforce

Emerging and advanced technologies are of little value without the skilled professionals that understand and can maximize their full potential. The FBI recognizes that the execution of FBI IT missions is driven by the collective talent, skills and capabilities of our IT professionals. As the FBI moves toward a consolidated and agile IT enterprise and implements policies and technologies necessary to support that transformation, the FBI will ensure that the critical success factors necessary to identify, develop and support the FBI IT workforce transformation are accounted for in IT strategic planning and execution.

Financial Challenges

The FBI, like other federal agencies, is facing significant challenges in funding its technology needs, while concurrently supporting the IT infrastructure and providing quality IT services. Upgrade initiatives require an infusion of budget dollars before initial cost savings from consolidation and retirement of systems are realized.

In compliance with DOJ directives, a four-year, rotating technical refresh plan for each of the major FBI IT areas is necessary. These areas include the FBINet, UNet and SCION network infrastructures and data centers. IT budgets need to reflect technical refresh initiatives to ensure IT is refreshed throughout the FBI and within a specified fiscal year. In order to achieve cost efficiencies, the FBI will require an integrated investment management approach, implementing disciplined cross-organizational funding decisions throughout the investment lifecycle, using best industry practices and performance based analysis.

The FBI IT governance processes, required from inception of business needs through the development of new investments and projects, are assisting the FBI to implement new IT capabilities in a controlled and orderly fashion.

Achieving the Vision

The FBI will draw on the IT goals and objectives outlined in the Strategic Goals and Objectives table for advancing the vision of future-state IT. Together, these goals and objectives make up the specific directives for the FBI's IT during 2010-2015. While these goals are kept at a high-level in this Strategic Plan, it is expected that individual projects and initiatives are necessary to execute against these planned goals. These projects and initiatives are in the ITB Strategic Budget submission and will be outlined in the Transition and Sequence Plans.

Goal 1 - Create a Resilient, Agile and Secure Infrastructure

The FBI IT will provide infrastructure updates, enterprise IT solutions, legacy mainframe application upgrades and/or replacement and utilize and reuse existing services where possible. The FBI will create an agile enterprise with evolution toward consolidated and shared infrastructure, services and applications. As part of the agile environment, the FBI will sustain a rigid information security management program, implementing tools and processes to enhance utilization of the EA through virtualization and abstraction. Strategically, the FBI will focus on fully understanding, adopting and integrating a shared services approach to IT and businesses challenges.

The FBI will actively defend information resources and critical infrastructures and provide assured information delivery, system and network access and information protection. The security and protection of our systems, networks and information depend on the implementation of sound information assurance concepts and principles across programs and platforms.

Objectives

1.1 Provide a comprehensive, resilient and modernized technical infrastructure with "right sized" Data Center(s) and Continuity of Operations (COOP) capabilities.

The FBI will intensify efforts to eliminate legacy networks, servers, systems, applications and duplicative data environments. The FBI will continue to transform silo and tightly coupled systems and applications into a set of enterprise services that emphasize a virtual environment of services and systems.

As an IT foundation, the FBI requires multiple data centers that are geographically dispersed and mutually supportive, providing requisite processing and storage capabilities to ensure availability of FBI mission critical services and data. Data center technology needs to consist of a modern, standardized IT infrastructure, including an Enterprise Hosting Environment that supports virtualization, remote access, a "lights out" operational posture and "green" technologies.

The FBI will standardize and deliver COOP and disaster recovery capabilities for timely and effective return of FBI mission critical IT systems to an operational state within a timeframe acceptable to the mission. An operational state includes recovery of data, applications and systems providing the IT service(s) required by the mission as well as the alternate facilities, recovery processes and the critical personnel supporting them. The institutional and corporate knowledge necessary to recover critical IT infrastructure should be dispersed in order to be as readily available as the systems themselves for standard operations, ensuring critical event continuity.

1.2 Enable user communication, collaboration and cross-domain information access through secure, enhanced and flexible networks.

The FBI will implement a unified communication strategy to increase service availability and transition to a unified communication posture. There are many technology services an enterprise may employ to perform its mission or reach its corporate goals, such as security services, web services, email, telecommunications, administrative services, metrics and unified communications. In formulating a convergence strategy, technologies need to be adaptable to the strategic goal of communicating with LE, IC and most importantly, throughout all FBI business units.

Unified Communications (UC) is an example of converging technologies. UC includes a variety of elements, such as instant messaging, telephony, video, email, voicemail and short message services, all of which can be brought into real time and coordinated. For example, with UC technology an agent or analyst could quickly locate a Subject Matter Expert within the FBI by accessing an interactive directory, engage in a text messaging session and then escalate the session to a voice call, or even a video call – all within minutes.

Voice over IP (VOIP) is not a new technology; however, it is maturing and becoming a more cost-effective alternative to conventional telephony systems. For the FBI to commit to a VoIP transformation, infrastructure upgrades will need to be in place along with expanded bandwidth accommodating VoIP and any associated and/or emerging VoIP technologies.

1.3 Provide enterprise users with standardized IT solutions and services using enhanced infrastructure support.

The FBI will provide highly reliable and available capabilities to users and decrease the time to deliver new capabilities. These enterprise services will be leveraged across the FBI to provide seamless connectivity to mission critical information, such as could be delivered with cloud computing. Cloud computing relates to the underlying architecture in which the services are hosted. The principle is that applications run somewhere in a "cloud" transparent to the user regarding location or implementation. With cloud computing, a user accesses an application using a thin client or other access point, with a personal device like an iPhone, BlackBerry, PC or laptop, reaching into the cloud for resources instead of being limited by what is resident on his/her localized device.

Goal 2 - Improve Analysis, Collaboration and Information Sharing

The FBI National Information Sharing Strategy (NISS) provides the common vision, goals and framework needed to guide information sharing initiatives with our federal, state, local and tribal agency partners; foreign government counterparts; and private sector stakeholders. The FBI utilized the guidelines of the National Strategy for Information Sharing for development and implementation of our National Information Sharing Strategy. The FBI NISS addresses the cultural and technological changes required to move the FBI to "a responsibility to provide" culture. The FBI will continue its transformation by identifying and adopting the best practices and evolving technology standards of both the intelligence and law enforcement communities to support collection, analysis, collaboration and dissemination. Additionally the FBI will develop ways to improve electronic discovery, disclosure and examination of data.

Objectives

2.1. Deploy Enterprise-wide Analytical capabilities.

The FBI IT providers will be active in partnership initiatives across FBI, participate in inter-agency boards and tiger teams and expand its role in business process improvement. The FBI will upgrade and integrate existing analytical capabilities and improve electronic discovery for all-source analysis to enhance analytic processes across the enterprise along with ingest, production and examination of intelligence data. To achieve these objectives the FBI will need to improve our processes to more effectively manage and deliver systems. Strategically, we will focus on fully understanding, adopting and integrating a shared services approach to IT and businesses challenges.

In order to meet these initiatives, the FBI will need to create, deploy and sustain an enterprise data management service. Improvements to the services to manage data, including management of data quality, are needed to provide for interoperable, standardized IT services, enterprise wide analytical capabilities, internal and external information sharing and deployment of information-based capabilities.

2.2. Advance Knowledge Management.

The FBI will continue to promote and institutionalize our Knowledge Management (KM) practices. KM is the cornerstone for decision making, knowledge sharing and information collaboration. Within the FBI, KM is the integration of people and processes, enabled by technology, to facilitate the exchange of operationally relevant information and expertise. KM can also improve enterprise-wide processes and improve the day-to-day operations at every level of the FBI.

2.3. Improve ability to provide timely and relevant information sharing with FBI, LE and IC partners.

The FBI will continually improve our IT capability to provide timely and relevant information sharing and collaboration services to LE and IC partners through an agile enterprise approach. The FBI will promote real time information sharing, collaboration and knowledge management. The FBI will improve information-to-operations through IT innovation that is relevant, timely and functional by leveraging emerging technologies and innovative reuse of existing technologies. The FBI will continuously discover and capture emerging or existing intelligence concepts, processes and technologies in collaboration with customers and industry partners through internal and inter-agency boards as partners in initiatives across FBI.

Goal 3 - Transform Our IT Workforce

The FBI will continue to expand the IT workforce initiatives in a manner that ensures that our staff is postured to execute current technologies, while ensuring effective and efficient use of emerging technologies and concepts. The CIO recognizes that the execution of the IT mission is driven by the collective talent, skills and capabilities of our IT professionals. As the FBI moves toward a resilient and agile IT environment and implements the policies and technologies necessary to support that transformation, we will account for the critical success factors necessary to identify, develop and support FBI IT employees.

Objectives

3.1. Become a center of excellence and employer of choice.

In conjunction with the FBI's Human Resources, we will identify and recruit top talent to close skill gaps and maximize the use of FBI resources to become a center of excellence and employer of choice. The FBI will transform our IT workforce to achieve operational excellence for improved customer service, communication and coordination.

3.2. Align workforce skills to achieve IT strategic goals and objectives.

The FBI will align IT staff skills to achieve IT strategic goals and objectives, increase CIO involvement in the recruitment process to better sustain the IT enterprise workforce, maintain an environment that fosters teamwork, collaboration and individual recognition and expand performance management practices that reward sustained excellence. The FBI will partner with business support areas to provide expertise and integrate efforts for enterprise solutions such as workflow, document/records management and collaboration tools.

3.3. Promote continuous learning and formal training programs for proactive skills development.

The FBI will promote and sustain a culture of continuous improvement, improve IT personnel management in concert with management of IT and establish a centralized view of workforce capabilities and skill requirements for continuous assessment, proactive management and employee career development.

Goal 4 - Improve the Overall Management of Information Technology

The FBI will continue to select effective and efficient IT business cases based on validated requirements where investments align with the FBI strategic objectives and priorities established in Presidential, Federal, DOJ and ODNI guidance. Where appropriate, IT investments will be interoperable within the DOJ, Intelligence Community and Law Enforcement collaborative environments. Portfolio Management and IT Governance will provide a standardized approach to determining return on investment and lifecycle costs across all programs before investment decisions are made. The FBI IT will develop service-based teams that ensure proper governance of IT projects and processes through customer advocacy initiatives.

Objectives

4.1. Provide enterprise solutions that support multiple mission areas.

In support of the mission, the FBI will develop innovative, mission-focused IT services, retire and replace legacy mainframe applications, deploy secure mobility and implement an unclassified and classified Voice over IP strategy. The FBI will leverage current and emerging technologies and science for innovative solutions, while refreshing older and useful technologies and reusing enterprise solutions such as SENTINEL content management, security and document/records management.

The FBI will increase the use of automated workflow tools, such as SENTINEL, to target information toward the people who need it and improve the IT product development cycle. This approach will create a more flexible work environment without sacrificing quality and cost of the products, while following

legislative mandates and federal departmental directives and policies. Workflow tools will also decrease silo and stove piped information thereby increasing information sharing and collaboration.

4.2. Leverage technology and science for innovative new solutions.

The FBI will enhance surveillance technologies along with their sustaining systems. The increased variety and complexity of advanced communication services and supporting technologies has impeded lawful intercept capabilities and created a "lawful intercept capabilities gap." The FBI must enhance electronic surveillance, collections, database consolidation, data presentation and analytic tools in order to meet the technology advancement challenges in all digital transmissions types and infrastructures. The FBI will also evolve existing biometric systems to be more effective and efficient.

4.3. Recommend IT solutions for enterprise services.

The FBI IT will enhance the delivery and management of enterprise-wide IT capabilities and services by leveraging proven practices, processes and standards and partnering with business support areas to provide service-based customer advocacy teams (enterprise human capital and financial solutions, etc.). The FBI will achieve an agile enterprise service delivery operating model to exploit and reuse existing services where possible and modernize legacy applications.

Server consolidation has been the traditional justification for virtualization and it remains an important factor. Virtualization technologies can provide significant benefits to the enterprise by pooling server resources to increase utilization and decrease capital expenditures. Through developing standard virtual server and workstation builds that are easily duplicated, virtualization will enable rapid deployment of server and application instances and provide significant flexibility in deploying multiple operating systems on a single hardware platform.

4.4. Optimize the FBI portfolio of IT resources (assets, projects, investments) through effective governance processes.

The FBI's IT Governance framework is a closed-loop system. It ensures investments are prioritized appropriately; that IT projects comply with the FBI's Life Cycle Management and good project management practices; ensures that IT decisions are made in a timely manner and at the right level; that IT projects are controlled and monitored appropriately; and that any corrective actions are swift. Ultimately, IT Governance is the primary means for the FBI to maintain continuous alignment among its IT investments, projects and the FBI's mission priorities. The FBI will improve Capital Planning and Investment Control processes to ensure that IT funds are well planned, cost-effective and strategically aligned with FBI, DOJ and ODNI goals and objectives.

In advancing the vision of future-state IT, the FBI will enhance our EA to support disciplined investment analysis by highlighting capability gaps and investment duplication, enhance processes, establish meaningful metrics and drive continuous improvement and accountability with an enterprise-wide performance management program. The FBI will ensure proper oversight and governance of IT projects and processes that maximize the effective and efficient use of FBI IT resources and employ integrated IT investment management capabilities to enable standardized, objective decision making that promotes investments to achieve mission outcomes.

Goal 5 - Enhance Customer Satisfaction

Information Technologies are "customer centric" tools and mission enablers. Whether our customers are internal (day-to-day operations) or external (LE, IC and/or other entities) we are committed to providing outstanding customer service to the greatest extent possible. We will endeavor to provide the right answers the first time and enhance our metrics to transparently gauge the effectiveness and efficiency of our customer service. We will assist in the development and administration of the Customer Satisfaction (CS) Processes to ensure IT is meeting our CS goals and objectives.

Objectives

5.1. Improve customer service, communication and coordination.

We will enhance IT customer management and provide relevant, timely and reliable enterprise capabilities and services that satisfy mission and customer needs.

5.2. Improve tracking, quality and timeliness of IT requests and customer service needs.

We will evaluate, enhance and drive efforts to improve the timeliness, quality and tracking of IT requests through employee training and customer understanding. Customer focus will shift from *closing requests* for assistance at the expense of IT performance statistics to *resolving issues* on first contact, where possible, with the proper and correct solution and follow-up to assure quality of service. We will evaluate and implement industry customer service best practice models such as blind surveys and pop-up surveys that provide feedback throughout the customer request cycle.

5.3. Increase Enterprise IT marketing efforts.

The FBI's IT will create a branding approach to affix to approved IT products. Once branded, our customers will be assured of the quality of our final product and the responsibility and pride of ownership associated with the IT. We will promote IT with concentration on "value added" services and customer relationship management. Our dictum will express our commitment to the customer and our pledge to provide quality IT solutions and technologies throughout the FBI.

Conclusion

The direction and theme of this plan revolves around remarks by FBI Director Mueller in discussing the new Field Intelligence Model, March 2008;

"It is more important, now than ever before, that we are ONE FBI. We cannot be 'stove piped' in any way – not by field office, not by region, or not by program. We are one enterprise, consisting of skilled professionals working together. Aided by cutting edge tools and technology, we will discover and create knowledge that provides early warning, directs operations, creates opportunities to further cases and informs national security policymakers."

Within the context of information technology, this statement holds true as well. With this ITSP providing guidance, the FBI is progressing toward an Agile Enterprise with a resilient and sustainable architecture which will be largely devoid of stove pipes and silo information networks. This transformation will allow the FBI to execute its mission, with leading edge technologies, while allowing emerging technology insertion, well into the 21st century.