United States General Accounting Office

GAO

Report to Congressional Requesters

September 2003

INFORMATION TECHNOLOGY

FBI Needs an Enterprise Architecture to Guide Its Modernization Activities

GAO-03-959

September 2003

INFORMATION TECHNOLOGY

FBI Needs an Enterprise Architecture to Guide Its Modernization Activities

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-03-959, a report to congressional requesters

Why GAO Did This Study

The Federal Bureau of Investigation (FBI) is in the process of modernizing its information technology (IT) systems. Replacing much of its 1980s-based technology with modern system applications and a robust technical infrastructure, this modernization is intended to enable the FBI to take an integrated approach—coordinated agencywide—to performing its critical missions, such as federal crime investigation and terrorism prevention. GAO was requested to conduct a series of reviews of the FBI's modernization management. The objective of this first review was to determine whether the FBI has an enterprise architecture to guide and constrain modernization investments.

What GAO Recommends

GAO recommends that the FBI Director designate the development of a complete enterprise architecture as a bureauwide priority and take the necessary steps to manage this development accordingly, including ensuring key enterprise architecture management practices specified in GAO's maturity framework are implemented.

We provided a draft of this report to the FBI on August 22, 2003, for its review and comment, but no comments were received in time for issuance of this final report.

www.gao.gov/cgi-bin/getrpt?GAO-03-959.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Randolph C. Hite at (202) 512-3439 or hiter@gao.gov.

What GAO Found

About 2 years into its ongoing systems modernization efforts, the FBI does not yet have an enterprise architecture. An enterprise architecture is an organizational blueprint that defines—in logical or business terms and in technology terms—how an organization operates today, intends to operate in the future, and intends to invest in technology to transition to this future state. GAO's research has shown that attempting to modernize an IT environment without a well-defined and enforceable enterprise architecture risks, among other things, building systems that do not effectively and efficiently support mission operations and performance.

The FBI acknowledges the need for an enterprise architecture and has committed to developing one by the fall of 2003. However, it currently lacks the means for effectively reaching this end. For example, while the bureau did recently designate a chief architect and select an architecture framework to use, it does not yet have an agency architecture policy, an architecture program management plan, or an architecture development methodology, all of which are necessary components of effective architecture management.

Given the state of the FBI's enterprise architecture management efforts, the bureau is at Stage 1 of GAO's enterprise architecture management maturity framework (see table). Organizations at Stage 1 are characterized by architecture efforts that are ad hoc and unstructured, lack institutional leadership and direction, and do not provide the management foundation necessary for successful architecture development and use as a tool for informed IT investment decision making. A key for an organization to advance beyond this stage is to treat architecture development, maintenance, and implementation as an institutional management priority, which the FBI has yet to do. To do less will expose the bureau's ongoing and planned modernization efforts to unnecessary risk.

GAO's Framework for Enterprise Architecture (EA) Management Maturity

Maturity stage	Description
Stage 1: Creating EA awareness	Organization does not have plans to develop and use an architecture, or its plans do not demonstrate an awareness of an architecture's value.
Stage 2: Building the EA management foundation	Organization recognizes EA as a corporate asset by vesting responsibility in an executive body with enterprisewide representation. It also develops plans for creating EA products and for measuring program progress and product quality and commits resources necessary to develop an EA.
Stage 3: Developing the EA	Organization is developing architecture products according to a framework, methodology, tool, and established management plans. EA products are not yet complete, but scope is defined and progress tracked.
Stage 4: Completing the EA	Organization has completed its EA products, which have been approved by management and verified by an independent agent. Further EA evolution is governed by a written EA maintenance policy.
Stage 5: Leveraging the EA to manage change	EA is being used by organization to manage and control IT investments, ensuring interoperability and avoiding overlap. Organization requires that investments comply with EA via written institutional policy. It also tracks and measures EA benefits or return on investment, adjusting EA management processes and products as needed.

Source: GAO.

Contents

Abbreviations

CIO	chief information officer
DNA	deoxyribonucleic acid
EA	enterprise architecture
FBI	Federal Bureau of Investigation
GAO	General Accounting Office
IT	information technology

This is a work of the U.S. government and is not subject to copyright protection in the United States. It may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

GAO
Accountability * Integrity * Reliability

United States General Accounting Office
Washington, D.C. 20548

September 25, 2003

The Honorable Porter J. Goss
Chairman, Permanent Select Committee on Intelligence
House of Representatives

The Honorable Nancy Pelosi
House of Representatives

The Honorable Bob Graham
United States Senate

The Honorable Richard C. Shelby
United States Senate

The Federal Bureau of Investigation (FBI) is in the process of modernizing its information technology (IT) systems. Its goal is to replace much of its 1980s-based IT environment to better support its plans for an agencywide approach to performing critical mission operations, including terrorism prevention and federal crime investigation. As you requested, we are conducting a series of reviews of the FBI's management of its modernization activities. The objective of this first review was to determine whether the FBI has a modernization blueprint, commonly called an enterprise architecture,[1] to guide and constrain its modernization efforts. Our research has shown that attempting to modernize an IT environment without a well-defined and enforceable enterprise architecture risks, among other things, building systems that do not effectively and efficiently support mission operations and performance. Details of our scope and methodology are in appendix I.

Results in Brief

The FBI does not have an enterprise architecture, although it began efforts to develop one about 32 months ago and has invested hundreds of millions of dollars in new systems over the last 2 years. Moreover, it does not yet have the means in place to effectively develop, maintain, and implement an enterprise architecture. That is, it does not have most of the architecture

[1]An enterprise architecture is a set of descriptive models (e.g., diagrams and tables) that define, in business terms and in technology terms, how an organization operates today, how it intends to operate in the future, and how it intends to invest in technology to transition from today's operational environment to tomorrow's.

management structures and processes advocated by federal guidance and best practices. For instance, the bureau does not have such architecture management controls as an agency architecture policy, an architecture program management plan, an architecture development methodology, and an automated architecture tool (a repository for architecture documentation).

Given the state of the FBI's enterprise architecture management efforts, the bureau has yet to advance beyond Stage 1, the beginning stage, of our best practices-based, five-stage enterprise architecture management maturity framework.[2] Organizations at Stage 1 are characterized by architecture efforts that are ad hoc and unstructured, lack institutional leadership and direction, and do not provide the management foundation necessary for successful architecture development and use for informed IT investment decision making. Key for an organization to advance beyond this stage is to first treat architecture development, maintenance, and implementation as an institutional management priority, which the FBI has yet to do, and to adopt architecture management best practices. To do less will continue to expose the bureau's ongoing and planned modernization efforts to unnecessary risk. Accordingly, we are making recommendations to the FBI's Director to assist in improving the bureau's enterprise architecture efforts. We provided a draft of this report to the FBI on August 22, 2003, for its review and comment, but no comments were received in time for issuance of this final report.

Background

The FBI was founded in 1908 to serve as the primary investigative bureau of the Department of Justice. Its mission includes upholding the law by investigating serious federal crimes; protecting the nation from foreign intelligence and terrorist threats; providing leadership and assistance to federal, state, local, and international law enforcement agencies; and being responsive to the public in the performance of these duties. Approximately 11,000 special agents and 16,000 professional support personnel are located at the bureau's Washington, D.C., headquarters and at more than 400 offices throughout the United States and 44 offices in foreign countries.

[2]U.S. General Accounting Office, *Information Technology: A Framework for Assessing and Improving Enterprise Architecture Management* (Version 1.1), GAO-03-584G (Washington, D.C.: April 2003).

Mission responsibilities at the bureau are divided among five major organizational components: Criminal Investigations, Law Enforcement Services, Counterterrorism and Counterintelligence, Intelligence, and Administration. Criminal Investigations, for example, investigates serious federal crimes, including those associated with organized crime, violent offenses, white-collar crime, government and business corruption, and civil rights infractions. It also probes federal statutory violations involving exploitation of the Internet and computer systems for criminal, foreign intelligence, and terrorism purposes. (The major components and their associated mission responsibilities are shown in table 1.) Each component is headed by an Executive Assistant Director who reports to the Deputy Director, who in turn reports to the Director.

To execute its mission responsibilities, the FBI relies on the use of IT. For example, it develops and maintains computerized IT systems such as the Combined DNA[3] Index System to support forensic examinations, the Digital Collection System to electronically collect information on known and suspected terrorists and criminals, and the National Crime Information Center and the Integrated Automated Fingerprint Identification System to help state and local law enforcement agencies identify criminals. According to FBI estimates, the bureau manages hundreds of systems, networks, databases, applications, and associated tools such as these at an average annual cost of about $800 million.

[3]Deoxyribonucleic acid.

Table 1: FBI Organizational Components and Mission Responsibilities

Component	Mission responsibilities
Criminal Investigations	Investigates serious federal crimes, including those associated with organized crime, violent offenses, white-collar crime, government and business corruption, and civil rights infractions
	Probes federal statutory violations involving exploitation of the Internet and computer systems for criminal, foreign intelligence, and terrorism purposes
Law Enforcement Services	Responds to and manages crisis incidents such as terrorist activities, child abductions, and other repetitive violent crimes
	Provides information services on fingerprint identification, stolen automobiles, criminals, crime statistics, and other information to state, local, and international law enforcement
	Performs forensic examinations in support of criminal investigations and prosecutions, including crime scene searches, DNA testing, photographic surveillance, expert court testimony, and other technical services
	Trains FBI agents and support personnel as well as state, local, international, and other federal law enforcement in crime investigation, law enforcement, and forensic investigative techniques
Counterterrorism and Counterintelligence	Identifies and neutralizes ongoing national security threats, including conducting foreign counterintelligence investigations, coordinates investigations within the U.S. intelligence community, and investigates violations of federal espionage statutes
	Assesses threats or attacks against critical U.S. infrastructure, issues warnings, and investigates and develops national responses to threats and attacks
Intelligence	Collects and analyzes information on evolving threats to the United States and ensures its dissemination within the FBI, to state and local law enforcement, and to the U.S. intelligence community
Administration	Develops and administers the bureau's personnel programs and services, including recruiting, conducting background investigations, and other administrative activities
	Administers the bureau's budget and fiscal matters, including financial planning, payroll services, property management, and procurement activities
	Manages and plans for the bureau's use of information resources
	Investigates allegations of criminal conduct and serious misconduct by FBI employees
	Manages policies, processes, and systems used by the bureau to control its extensive investigative and other records
	Ensures a safe and secure FBI work environment, including preventing the compromise of national security and FBI information

Source: GAO based on FBI data.

FBI's Existing IT Environment Has Long Suffered from Known Deficiencies

Several prior reviews of the FBI's existing IT environment have revealed that it is antiquated and not integrated. Specifically, the Department of Justice Inspector General reported[4] that as of September 2000, the FBI had over 13,000 desktop computers that were 4 to 8 years old and could not run basic software packages. Moreover, it reported that some communications networks were 12 years old and obsolete, and that many end-user applications existed that were neither Web-enabled nor user-friendly. In addition, a December 2001 review initiated by the Department of Justice[5] found that FBI's IT environment was disparate. In particular, it identified 234 nonintegrated ("stove-piped") applications, residing on 187 different servers, each of which had its own unique databases and did not share information with other applications or with other government agencies. Moreover, in June 2002, we reported[6] that IT has been a long-standing problem for the bureau, involving outdated hardware, outdated software, and the lack of a fully functional E-mail system. We also reported that these deficiencies served to significantly hamper the FBI's ability to share important and time-sensitive information internally and externally with other intelligence and law enforcement agencies.

FBI Has Initiated a Large, Complex Systems Modernization

Following the terrorist attacks of September 11, 2001, the FBI refocused its efforts to investigate the events and to detect and prevent possible future attacks. To do this, the bureau changed its priorities and accelerated modernization of its IT systems. Collectively, the FBI's many modernization efforts involve 51 initiatives that the FBI reported will cost about $1.5 billion between fiscal years 2002 and 2004. For example, the Trilogy project, which is to introduce new systems infrastructure and applications, includes establishing an enterprisewide network to enable communications between hundreds of FBI locations domestically and abroad, upgrading 20,000 desktop computers, and providing 2,400 printers and 1,200 scanners. In addition, a new investigative data warehousing initiative called Secure Counterterrorism Operational Prototype

[4]U.S. Department of Justice Office of the Inspector General, *Federal Bureau of Investigation's Management of Information Technology Investments*, Report 03-09 (Washington, D.C.: December 2002).

[5]Arthur Andersen, LLP, *Management Study of the Federal Bureau of Investigation* (Dec. 14, 2001).

[6]U.S. General Accounting Office, *FBI Reorganization: Initial Steps Encouraging but Broad Transformation Needed*, GAO-02-865T (Washington, D.C.: June 21, 2002).

Environment is to (1) aggregate voluminous counterterrorism files obtained from both internal and external sources and (2) acquire analytical capabilities to improve the FBI's ability to analyze these files. Another initiative, called the FBI Administrative Support System, is to integrate the bureau's financial management and administrative systems with the Department of Justice's new financial management system.

Beyond the scope and size of the FBI's modernization effort is the need to ensure that the modernized systems effectively support information sharing within the bureau and among its law enforcement and intelligence community partners. This means that the modernized FBI systems will, in many cases, have to interface with existing (legacy) systems to obtain data to accomplish their functions, which bureau officials said will be challenging, given the nonstandard and disparate nature of the existing IT environment. Moreover, bureau staff will have to be trained on the new systems and business processes modified to accommodate their use.

An Enterprise Architecture Is Essential to Effectively Managing Systems Modernization

The development, maintenance, and implementation of enterprise architectures (EA) are recognized hallmarks of successful public and private organizations and as such are an IT management best practice. EAs are essential to effectively managing large and complex system modernization programs, such as the FBI's. Our experience with federal agencies has shown that attempting a major modernization effort without a well-defined and enforceable EA results in systems that are duplicative, are not well integrated, are unnecessarily costly to maintain and interface, and do not effectively optimize mission performance.[7]

The Congress and the Office of Management and Budget have recognized the importance of agency EAs. The Clinger-Cohen Act, for example, requires that agency Chief Information Officers (CIO) develop, maintain, and facilitate the implementation of architectures as a means of integrating

[7]See, for example, U.S. General Accounting Office, *DOD Business Systems Modernization: Improvements to Enterprise Architecture Development and Implementation Efforts Needed*, GAO-03-458 (Washington, D.C.: February 2003); *Information Technology: DLA Should Strengthen Business Systems Modernization Architecture and Investment Activities*, GAO-01-631 (Washington, D.C.: June 2001); and *Information Technology: INS Needs to Better Manage the Development of Its Enterprise Architecture*, GAO/AIMD-00-212 (Washington, D.C.: August 2000).

business processes and agency goals with IT.[8] In response to the act, the Office of Management and Budget, in collaboration with us and others, has issued guidance on the development and implementation of these architectures.[9] It has also issued guidance that requires agency investments in information systems to be consistent with agency architectures.[10]

An EA is a systematically derived snapshot—in useful models, diagrams, and narrative—of a given entity's operations (business and systems), including how its operations are performed, what information and technology are used to perform the operations, where the operations are performed, who performs them, and when and why they are performed. The architecture describes the entity in both logical terms (e.g., interrelated functions, information needs and flows, work locations, systems, and applications) and technical terms (e.g., hardware, software, data, communications, and security). EAs provide these perspectives for both the entity's current (or "as-is") environment and for its target (or "to-be") environment; they also provide a high-level capital investment roadmap for moving from one environment to the other.

Among others, the Office of Management and Budget, the National Institute of Standards and Technology, and the federal CIO Council have issued frameworks that define the scope and content of architectures.[11] For example, the federal CIO Council issued a framework, known as the *Federal Enterprise Architecture Framework*, in 1999. While the various frameworks differ in their nomenclatures and modeling approaches, they consistently provide for defining an enterprise architecture's operations in both logical terms and technical terms and providing these perspectives both for the "as-is" and "to-be" environments, as well as the investment roadmap. Managed properly, an enterprise architecture can clarify and help optimize the interdependencies and relationships among a given entity's

[8]40 U.S.C. 111315(b)(2).

[9]Office of Management and Budget, *Information Technology Architectures*, Memorandum M-97-16 (June 18, 1997), rescinded with the update of Office of Management and Budget Circular A-130 (Nov. 30, 2000).

[10]Office of Management and Budget, *Management of Federal Information Resources*, Circular A-130 (Nov. 30, 2000).

[11]Office of Management and Budget Circular A-130; National Institute of Standards and Technology, *Information Management Directions: The Integration Challenge*, Special Publication 500-167 (September 1989); and federal CIO Council, *Federal Enterprise Architecture Framework*, Version 1.1 (September 1999).

business operations and the underlying systems and technical infrastructure that support these operations.

The FBI's Lack of an EA Has Been Previously Reported

Over the past few years, several reviews related to the FBI's management of its IT have focused on enterprise architecture efforts and needs. For example, in July 2001, the Department of Justice hired a consulting firm to review the FBI's IT management. Among other things, the consultant recommended that the bureau develop a comprehensive EA to help reduce the proliferation of disparate, noncommunicating applications.[12]

The next year, in February 2002, we reported as part of a governmentwide survey of the state of EA maturity that the FBI was one of a number of federal agencies that were not effectively managing their architecture efforts, and we made recommendations to the Office of Management and Budget for advancing the state of architecture maturity across the federal government.[13] In this report, we noted that while the FBI was attempting to lay the management foundation for developing an architecture, the bureau had not yet established certain basic management structures and controls, such as establishing a steering committee or group that had responsibility for directing and overseeing the development of the architecture.

Later, our June 2002 testimony[14] recommended that the FBI significantly upgrade its IT management capabilities, including developing an architecture, in order to successfully change its mission and effectively transform itself. Subsequently, in December 2002, the Department of Justice Inspector General reported[15] that the FBI needed to complete an architecture to complement its IT investment management processes.

[12]Arthur Andersen, LLP, *Management Study of the Federal Bureau of Investigation* (Dec. 14, 2001).

[13]U.S. General Accounting Office, *Information Technology: Enterprise Architecture Use Across the Federal Government Can Be Improved*, GAO-02-6 (Washington, D.C.: Feb. 19, 2002).

[14]GAO-02-865T.

[15]U.S. Department of Justice Office of the Inspector General, *Federal Bureau of Investigation's Management of Information Technology Investments*, Report 03-09 (Washington, D.C.: December 2002).

GAO's EA Management Maturity Framework Provides a Tool for Measuring and Improving EA Management Effectiveness

According to guidance published by the federal CIO Council,[16] effective architecture management consists of a number of key practices and conditions (e.g., establishing a governance structure, developing policy, defining management plans, and developing and issuing an architecture). In April 2003, we published a maturity framework that arranges these key practices and conditions (i.e., core elements) of the council's guide into five hierarchical stages, with Stage 1 representing the least mature and Stage 5 being the most mature.[17] The framework provides an explicit benchmark for gauging the effectiveness of EA management and provides a roadmap for making improvements. Each of the five stages is described below.

1. *Creating EA awareness.* The organization does not have plans to develop and use an architecture, or it has plans that do not demonstrate an awareness of the value of having and using an architecture. While Stage 1 agencies may have initiated some EA activity, these agencies' efforts are ad hoc and unstructured, lack institutional leadership and direction, and do not provide the management foundation necessary for successful EA development.

2. *Building the EA management foundation.* The organization recognizes that the EA is a corporate asset by vesting accountability for it in an executive body that represents the entire enterprise. At this stage, an organization assigns EA management roles and responsibilities and establishes plans for developing EA products and for measuring program progress and product quality; it also commits the resources necessary for developing an architecture—people, processes, and tools.

3. *Developing the EA.* The organization focuses on developing architecture products according to the selected framework, methodology, tool, and established management plans. Roles and responsibilities assigned in the previous stage are in place, and resources are being applied to develop actual EA products. The scope of the architecture has been defined to encompass the entire enterprise, whether organization-based or function-based.

[16]Federal CIO Council, *A Practical Guide to Federal Enterprise Architecture*, Version 1.0 (February 2001).

[17]GAO-03-584G.

4. *Completing the EA.* The organization has completed its EA products, meaning that the products have been approved by the EA steering committee or an investment review board, and by the CIO. Further, an independent agent has assessed the quality (i.e., completeness and accuracy) of the EA products. Additionally, evolution of the approved products is governed by a written EA maintenance policy approved by the head of the organization.

5. *Leveraging the EA to manage change.* The organization has secured senior leadership approval of the EA products and has a written institutional policy stating that IT investments must comply with the architecture, unless granted an explicit compliance waiver. Further, decision makers are using the architecture to identify and address ongoing and proposed IT investments that are conflicting, overlapping, not strategically linked, or redundant. Also, the organization tracks and measures EA benefits or return on investment, and adjustments are continuously made to both the EA management process and the EA products.

FBI Does Not Have an EA or the Management Foundation Needed to Effectively Develop, Maintain, and Implement One

The FBI has yet to develop an EA, and it does not have the requisite means in place to effectively develop, maintain, and implement one. The state of the bureau's architecture efforts is attributable to the level of management priority and commitment that the bureau has assigned to this effort. Unless this changes, it is unlikely the FBI will produce a complete and useful architecture, and without the architecture, the bureau will be severely challenged in its ability to implement a set of modernized systems that optimally support critical mission needs.

FBI Does Not Have an Architecture

An EA is an essential tool for effectively and efficiently engineering business operations (e.g., processes, work locations, and information needs and flows) and defining, implementing, and evolving IT systems in a way that best supports these operations. As mentioned earlier, an EA provides systematically derived and captured structural descriptions—in useful models, diagrams, tables, and narrative—of how a given entity operates today and how it plans to operate in the future, and it includes a roadmap for transitioning from today to tomorrow. The nature and content of these descriptions vary among organizations depending on the EA framework selected.

The FBI has selected the federal CIO Council's *Federal Enterprise Architecture Framework* as the basis for defining its EA. At the highest level of component content description, the *Federal Enterprise Architecture Framework* requires an "as-is" architectural description, a "to-be" architectural description, and a transition plan. For the "as-is" and "to-be" descriptions, this framework also requires the following major architecture products: business, information/data, applications, and technical components.

The FBI has yet to develop any of these architectural components. In response to our requests for all EA products, FBI officials, including the chief architect and the deputy chief information officer, told us that they do not yet exist. They added that they are currently in the process of developing an inventory of the FBI's existing (legacy) systems, which is a first step toward creating "as-is" architectural descriptions. They also stated that their goal is to develop and issue an initial bureau EA by the fall of 2003.

The FBI lacks an architecture largely because it is not treating development and use of one as a management priority. According to the FBI's chief architect, although the FBI launched its architecture effort 32 months ago, resources allocated to this effort have been limited to about $1 million annually and four staff. In contrast, our research of successful architecture efforts in other federal agencies shows that their resource needs are considerably greater than those that the FBI has committed. Similarly, the Justice Inspector General reported in December 2002[18] that limited funding and resources contributed to the immature state of the bureau's EA efforts. Additionally, assignment of responsibility and accountability for developing the architecture has not been stable over the last 32 months. For example, the chief architect has changed three times in the past 12 months.

As our prior reviews of federal agencies and research of architecture best practices show, attempts to modernize systems without an architecture, which is what the FBI is doing, increases the risk that large sums of money and much time and effort will be invested in technology solutions that are duplicative, are not well integrated, are unnecessarily costly to maintain and interface, and do not effectively optimize mission performance. In the

[18]U.S. Department of Justice Office of the Inspector General, *Federal Bureau of Investigation's Management of Information Technology Investments*, Report 03-09 (Washington, D.C.: December 2002).

FBI's case, there are indications that this is occurring. For example, the director of the modernization program management office told us that the office recently assumed responsibility for managing three system modernization initiatives[19] and found that they will require rework in order for them to be integrated. Such integration—which an EA would have provided for—was not previously factored into their development.

To allow for a more coordinated and integrated approach to pursuing its other 48 modernization initiatives, the FBI has started holding informal meetings among top managers to discuss related systems. However, such meetings are not a sufficient surrogate for an explicitly defined architectural blueprint that provides a commonly understood, accepted frame of reference against which to effectively and efficiently acquire and implement well-integrated systems.

Management Structures and Processes Needed to Develop, Maintain, and Implement an EA Are Not In Place

Because the task of developing, maintaining, and implementing an EA is an important, complex, and difficult endeavor, doing so effectively and efficiently requires that rigorous, disciplined management practices be adopted. Such practices form the basis of our EA management maturity framework, which specifies by stages the key architecture management structures, processes, and controls that are embodied in federal guidance and best practices. For example, Stage 2 specifies nine key practices or core elements that are necessary to provide the management foundation for successfully launching and sustaining an architecture effort. Five of the nine Stage 2 core elements are described below.

- *Establish an architecture steering committee representing the enterprise and make the committee responsible for directing, overseeing, or approving the EA.* This committee should include executive-level representatives from each line of business, and these representatives should have the authority to commit resources and enforce decisions within their respective organizational units. By establishing this enterprisewide responsibility and accountability, the agency demonstrates its commitment to building the management foundation and obtaining buy-in from across the organization.

[19]The three modernized systems that the program management office is integrating are Trilogy, Secure Counterterrorism Operational Prototype Environment, and FBI Administrative Support System.

- *Appoint a chief architect who is responsible and accountable for the EA, and who is supported by the EA program office and overseen by the architecture steering committee.* The chief architect, in collaboration with the Chief Information Officer, the architecture steering committee, and the organizational head, is instrumental in obtaining organizational buy-in for the EA, including support from the business units, as well as in securing resources to support architecture management functions, such as risk management, configuration management, quality assurance, and security management.

- *Use an architecture development framework, methodology, and automated tool to develop and maintain the EA.* These are important because they provide the means for developing the architecture in a consistent and efficient manner. The framework provides a formal structure for representing the EA, while the methodology is the common set of procedures that the enterprise is to follow in developing the EA products. The automated tool serves as a repository where architectural products are captured, stored, and maintained.

- *Develop an architecture program management plan.* This plan specifies how and when the architecture is to be developed. It includes a detailed work breakdown structure, resource estimates (e.g., funding, staffing, and training), performance measures, and management controls for developing and maintaining the architecture. The plan demonstrates the organization's commitment to managing EA development and maintenance as a formal program.

- *Allocate adequate resources to the EA effort.* An organization needs to have the resources (funding, people, tools, and technology) to establish and effectively manage its architecture. This includes, among other things, identifying and securing adequate funding to support EA activities, hiring and retaining the right people, and selecting and acquiring the right tools and technology to support activities.

Our framework similarly identifies key architecture management practices associated with later stages of EA management maturity. For example, at Stage 3, the stage at which organizations focus on architecture development activities, organizations need to satisfy six core elements. Two of the six are discussed below.

- *Issue a documented architecture policy, approved by the organization's head, governing the development of the EA.* The policy

defines the scope of the architecture, including the requirement for a description of the baseline and target architecture, as well as an investment roadmap or sequencing plan specifying the move between the two. This policy is an important means for ensuring enterprisewide commitment to developing an EA and for clearly assigning responsibility for doing so.

- *Ensure that EA products are under configuration management.* This involves ensuring that changes to products are identified, tracked, monitored, documented, reported, and audited. Configuration management maintains the integrity and consistency of products, which is key to enabling effective integration among related products and for ensuring alignment between architecture artifacts.

At Stage 4, during which organizations focus on architecture completion activities, organizations need to satisfy eight core elements. Two of the eight are described below.

- *Ensure that EA products and management processes undergo independent verification and validation.* This core element involves having an independent third party—such as an internal audit function or contractor that is not involved with any of the architecture development activities—verify and validate that the products were developed in accordance with EA processes and product standards. Doing so provides organizations with needed assurance of the quality of the architecture.

- *Ensure that business, performance, information/data, application/service, and technology descriptions address security.* An organization should explicitly and consistently address security in its business, performance, information/data, application/service, and technology EA products. Because security permeates every aspect of an organization's operations, the nature and substance of institutionalized security requirements, controls, and standards should be captured in EA products.

At Stage 5, during which the focus is on architecture maintenance and implementation activities, organizations need to satisfy eight core elements. Two of the eight are described below.

- *Make EA an integral component of IT investment decision-making processes.* Because the roadmap defines the IT systems that an

organization plans to invest in as it transitions from the "as-is" to the "to-be" environment, the EA is a critical frame of reference for making IT investment decisions. Using the EA when making such decisions is important because organizations should approve only those investments that move the organization toward the "to-be" environment, as specified in the roadmap.

- *Measure and report return on EA investment.* Like any investment, the EA should produce a return on investment (i.e., a set of benefits), and this return should be measured and reported in relation to costs. Measuring return on investment is important to ensure that expected benefits from the EA are realized and to share this information with executive decision makers, who can then take corrective action to address deviations from expectations.

Effective EA management is generally not achieved until an organization has a completed and approved architecture that is being effectively maintained and implemented, which is equivalent to having satisfied many Stage 4 and 5 core elements. Table 2 summarizes our framework's five stages and the associated core elements for each.

Table 2: Summary of GAO EA Management Framework Maturity Stages and Core Elements

Stage	Core elements
Stage 1: Creating EA awareness	Agency is aware of EA.
Stage 2: Building the EA management foundation	Adequate resources exist.
	Committee or group representing the enterprise is responsible for directing, overseeing, or approving EA.
	Program office responsible for EA development and maintenance exists.
	Chief architect exists.
	EA is being developed using a framework, methodology, and an automated tool.
	EA plans call for describing "as-is" environment, "to-be" environment, and sequencing plan.
	EA plans call for describing the enterprise in terms of business, data, applications, and technology.
	EA plans call for business, performance, data, applications, and technology descriptions to address security.
	EA plans call for developing metrics for measuring EA progress, quality, compliance, and return on investment.

(Continued From Previous Page)

Stage	Core elements
Stage 3: Developing EA products (includes all elements from Stage 2)	Written/approved policy exists for EA development.
	EA products are under configuration management.
	EA products describe *or will describe* the enterprise's business—and the data, applications, *and* technology that support it.
	EA products describe *or will describe* the "as-is" environment, the "to-be" environment, *and* a sequencing plan.
	Business, performance, data, application, and technology address *or will address* security.
	Progress against EA plans is measured and reported.
Stage 4: Completing EA products (includes all elements from Stage 3)	Written/approved policy exists for EA maintenance.
	EA products and management processes undergo independent verification and validation.
	EA products describe the enterprise's business—and the data, applications, *and* technology that support it.
	EA products describe the "as-is" environment, the "to-be" environment, and a sequencing plan.
	Business, performance, data, application, and technology descriptions address security.
	Organization chief information officer has approved EA.
	Committee or group representing the enterprise or the investment review board has approved current version of EA.
	Quality of EA products is measured and reported.
Stage 5: Leveraging the EA for managing change (includes all elements from Stage 4)	Written/approved policy exists for IT investment compliance with EA.
	Process exists to formally manage EA change.
	EA is integral component of IT investment management process.
	EA products are periodically updated.
	IT investments comply with EA.
	Organization head has approved current version of EA.
	Return on EA investment is measured and reported.
	Compliance with EA is measured and reported.

Source: GAO.

The FBI is currently at Stage 1 of our maturity framework. Of the nine foundational stage core elements (Stage 2), the FBI has fully satisfied one element by designating a chief architect. Additionally, the bureau has partially satisfied two other elements. First, it has established an architecture governance board as its steering committee. However, the bureau has not included all relevant FBI stakeholders on the board, such as representatives from its counterterrorism and counterintelligence organizational component. Second, the bureau has selected the *Federal Enterprise Architecture Framework* as the framework to guide its architecture development. However, it has not yet selected a development methodology or automated tool (a repository for architectural products).

The FBI has not satisfied the six remaining Stage 2 core elements. For example, the bureau has not established a program office. In addition, it has not developed a program management plan that provides for describing (1) the bureau's "as-is" and "to-be" environments, as well as a sequencing plan for transitioning from the "as-is" to the "to-be" and (2) the enterprise in terms of business, data, applications and technology, including how security will be addressed in each. With respect to Stages 3, 4, and 5, the FBI has not satisfied any of the associated core elements. (The detailed results of our assessment of the FBI's satisfaction of each of the stages and associated core elements is provided in app. II.)

The state of the FBI's EA management maturity is attributable to a lack of management commitment to having and using an architecture and to giving it priority. Indeed, several of the core elements cited above as not being satisfied, such as having EA policies and allocating adequate resources, are indicators of an organization's architectural commitment. According to FBI officials, including the chief architect, EA management has not been an agency priority, and thus has not received needed attention and resources.

Without effective EA management structures, processes, and controls, it is unlikely that the bureau will be able to produce a complete and enforceable enterprise architecture and thus be able to implement modernized systems in a way that minimizes overlap and duplication and maximizes integration and mission support.

Conclusions

The bureau's ongoing and planned system modernization efforts are at risk of not being defined and implemented in a way that best supports institutional mission needs and operations. Effectively mitigating this risk will require swift development and use of a modernization blueprint, or enterprise architecture; up to now, the FBI has not adequately demonstrated a commitment to developing such an architecture. In reversing this pattern, it is important that the architecture development and use be made an agency priority, and that it be managed in a way that satisfies the practices embodied in our architecture management maturity framework. To do less will continue to expose the bureau's system modernization efforts, and ultimately the effectiveness and efficiency of its mission performance, to unnecessary risk.

Recommendations

We recommend that the FBI Director immediately designate EA development, maintenance, and implementation as an agency priority and manage it as such. To this end, we recommend that the Director ensure that appropriate steps are taken to develop, maintain, and implement an EA in a manner consistent with our architecture management framework. This includes first laying an effective EA management foundation by (1) ensuring that all business partners are represented on the architecture governance board; (2) adopting an architecture development methodology and automated tool; (3) establishing an EA program office that is accountable for developing the EA; (4) tasking the program office with developing a management plan that specifies how and when the EA is to be developed and issued; (5) ensuring that the management plan provides for the bureau's "as-is" and "to-be" environments, as well as a sequencing plan for transitioning from the "as-is" to the "to-be"; (6) ensuring that the management plan also describes the enterprise in terms of business, data, applications, and technology; (7) ensuring that the plan also calls for describing the security related to the business, data, and technology; (8) ensuring that the plan establishes metrics for measuring EA progress, quality, compliance, and return on investment; and (9) allocating the necessary funding and personnel to EA activities.

Next, we recommend that the Director ensure that steps to develop the architecture products include (1) establishing a written and approved policy for EA development; (2) placing EA products under configuration management; (3) ensuring that EA products describe the enterprise's business, as well as the data, applications, and technology that support it; (4) ensuring that EA products describe the "as-is" environment, the "to-be" environment, and a sequencing plan; (5) ensuring that business, performance, data, application, and technology descriptions address security; and (6) ensuring that progress against EA plans is measured and reported.

In addition, we recommend that the Director ensure that steps to complete architecture products include (1) establishing a written and approved policy for EA maintenance; (2) ensuring that EA products and management processes undergo independent verification and validation; (3) ensuring that EA products describe the enterprise's business and the data, application, and technology that supports it; (4) ensuring that EA products describe the "as-is" environment, the "to-be" environment, and a sequencing plan; (5) ensuring that business, performance, data, application, and technology descriptions address security; (6) ensuring that

the Chief Information Officer approves the EA; (7) ensuring that the steering committee and/or the investment review board has approved the current version of the EA; and (8) measuring and reporting on the quality of EA products.

Further, we recommend that the Director ensure that steps taken to use the EA to manage modernization efforts include (1) establishing a written and approved policy for IT investment compliance with EA, (2) establishing processes to formally manage EA changes, (3) ensuring that EA is an integral component of IT investment management processes, (4) ensuring that EA products are periodically updated, (5) ensuring that IT investments comply with the EA, (6) obtaining Director approval of the current EA version, (7) measuring and reporting EA return on investment, and (8) measuring and reporting on EA compliance.

Finally, we recommend that the Director ensure that the bureau develops and implements an agency strategy for mitigating the risks associated with continued investment in modernized systems before it has an EA and controls for implementing it.

Agency Comments

We discussed our findings with the FBI's Chief Architect and later transmitted a draft of this report to the bureau on August 22, 2003, for its review and comment, requesting that any comments be provided by September 18, 2003. However, none were provided in time to be included in this printed report.

We are sending copies of this report to the Chairman and Vice Chairman of the Senate Select Committee on Intelligence and the Ranking Minority Member of the House Permanent Select Committee on Intelligence. We are also sending copies to the Attorney General; the Director, FBI; the Director, Office of Management and Budget; and other interested parties. In addition, the report will also be available without charge on GAO's Web site at http://www.gao.gov.

Should you have any questions about matters discussed in this report, please contact me at (202) 512-3439 or by E-mail at hiter@gao.gov. Key contributors to this report are listed in appendix III.

Randolph C. Hite
Director, Information Technology Architecture
and Systems Issues

Scope and Methodology

To evaluate whether Federal Bureau of Investigation (FBI) has a modernization blueprint, commonly called an enterprise architecture (EA), to guide and constrain its modernization efforts, we requested that the bureau provide us with all of its EA products. We also interviewed FBI officials, including the chief architect, to verify the status and plans for developing bureau EA products, the causes for why none had been completed to date, and the effects of proceeding with modernization initiatives without an EA.

To assess whether the FBI was effectively managing its architecture activities, we compared bureau EA management practices to our EA management maturity framework.[1] This framework is based on *A Practical Guide to Federal Enterprise Architecture*, published by the federal Chief Information Officers (CIO) Council.[2] To do this, we first reviewed bureau EA plans and products, and we interviewed FBI officials to verify and clarify our understanding of bureau EA efforts. Next, we compared the information that we had collected against our EA management maturity framework practices to determine the extent to which the FBI was employing such effective management practices. In addition, we interviewed FBI's chief architect and other bureau officials to determine, among other things, the cause of differences between what is specified in the framework and the condition at the FBI. We also reviewed past FBI information technology (IT) management studies and Department of Justice Inspector General reports, to understand the state of FBI management practices, including their strengths and weaknesses, underlying causes for improvements, and open recommendations. Further, we interviewed FBI division officials to understand the extent of their participation in the bureau's architecture efforts. Finally, to verify our findings and validate our assessment, we discussed with the chief architect our analysis of the state of FBI's EA practices against our maturity framework.

We performed our work at FBI headquarters in Washington, D.C., from September 2002 until August 2003, in accordance with generally accepted government auditing standards.

[1]U.S. General Accounting Office, *Information Technology: Enterprise Architecture Use Across the Federal Government Can Be Improved*, GAO-02-6 (Washington, D.C.: Feb. 19, 2002).

[2]Federal CIO Council, *A Practical Guide to Federal Enterprise Architecture*, Version 1.0 (February 2001).

Assessment of FBI's Enterprise Architecture (EA) Efforts against GAO's EA Management Maturity Framework

Stage	Core elements	Satisfied? (yes, no, or partially)	Comments
Stage 1: Creating EA awareness	Agency is aware of EA.	Yes	The FBI has acknowledged the need for an EA.
Stage 2: Building the EA management foundation	Adequate resources exist.	No	The FBI has allocated four architects and approximately $1 million annually for the development, implementation, and maintenance of its EA.
	Committee or group representing the enterprise is responsible for directing, overseeing, or approving EA.	Partially	The FBI has established the architecture governance board to direct, oversee, and approve the EA. However, not all FBI components are represented on the board.
	Program office responsible for EA development and maintenance exists.	No	The FBI does not have a program office responsible for the development, maintenance, or implementation of its EA.
	Chief architect exists.	Yes	The FBI has designated a chief architect.
	EA is being developed using a framework, methodology, and an automated tool.	Partially	The FBI plans to use the Federal Enterprise Architecture Framework. However, FBI officials reported that they are not using a methodology or automated tool.
	EA plans call for describing "as-is" environment, "to-be" environment, and sequencing plan.	No	No EA plans exist.
	EA plans call for describing the enterprise in terms of business, data, applications, and technology.	No	No plans exist.
	EA plans call for business, performance, data, application, and technology descriptions to address security.	No	No plans exist.
	EA plans call for developing metrics for measuring EA progress, quality, compliance, and return on investment.	No	No plans exist.

(Continued From Previous Page)

Stage	Core elements	Satisfied? (yes, no, or partially)	Comments
Stage 3: Developing EA products (includes all elements from Stage 2)	Written/approved policy exists for EA development.	No	The FBI does not have a written and approved policy for EA development.
	EA products are under configuration management.	No	The FBI has not developed its EA products; thus no products are under configuration management.
	EA products describe or will describe the enterprise's business and the data, applications, and technology that support it.	No	The FBI plans to describe its enterprise's business and the data, applications, and technology that support it. However, no completion date has been established.
	EA products describe or will describe the "as-is" environment, the "to-be" environment, and a sequencing plan.	No	The FBI plans to describe its "as-is" and "to-be" environments, as well as a sequencing plan. However, no completion date has been established.
	Business, performance, data, application, and technology address or will address security.	No	No plans exist.
	Progress against EA plans is measured and reported.	No	No plans exist.
Stage 4: Completing EA products (includes all elements from Stage 3)	Written/approved policy exists for EA maintenance.	No	According to FBI officials, there is no written and approved policy for EA maintenance.
	EA products and management processes undergo independent verification and validation.	No	The FBI has not developed EA products, and management processes do not undergo independent verification and validation.
	EA products describe the enterprise's business and the data, applications, and technology that support it.	No	The FBI has not developed these products.
	EA products describe the "as-is" environment, the "to-be" environment, and a transitioning plan.	No	The FBI has not developed these products.
	Business, performance, data, application, and technology descriptions address security.	No	No plans exist.
	Organization chief information officer has approved EA.	No	There is no approved version of the FBI's EA.
	Committee or group representing the enterprise or the investment review board has approved current version of EA.	No	The FBI has not developed an EA.
	Quality of EA products is measured and reported.	No	The FBI has not developed an EA.

(Continued From Previous Page)

Stage	Core elements	Satisfied? (yes, no, or partially)	Comments
Stage 5: Leveraging the EA for managing change (includes all elements from Stage 4)	Written/approved policy exists for IT investment compliance with EA.	No	The FBI has no written and approved policy addressing IT investment compliance with EA.
	Process exists to formally manage EA change.	No	No management plans exist.
	EA is integral component of IT investment management process.	No	The FBI has not developed an EA.
	EA products are periodically updated.	No	The FBI has not developed an EA.
	IT investments comply with EA.	No	The FBI has not developed an EA.
	Organization head has approved current version of EA.	No	The organization head has not approved the EA.
	Return on EA investment is measured and reported.	No	The FBI does not have an EA to determine return on investment.
	Compliance with EA is measured and reported.	No	The FBI does not have an EA to measure and report compliance.

Source: GAO based on FBI data.

GAO Contact and Staff Acknowledgments

GAO Contact

Gary Mountjoy, (202) 512-6367

Acknowledgments

In addition to the individual named above, key contributors to this report included Nabajyoti Barkakati, Katherine I. Chu-Hickman, Barbara Collier, Michael Fruitman, David Hinchman, Mary Beth McClanahan, Paula Moore, and Megan Secrest.

GAO's Mission

The General Accounting Office, the audit, evaluation and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through the Internet. GAO's Web site (www.gao.gov) contains abstracts and full-text files of current reports and testimony and an expanding archive of older products. The Web site features a search engine to help you locate documents using key words and phrases. You can print these documents in their entirety, including charts and other graphics.

Each day, GAO issues a list of newly released reports, testimony, and correspondence. GAO posts this list, known as "Today's Reports," on its Web site daily. The list contains links to the full-text document files. To have GAO e-mail this list to you every afternoon, go to www.gao.gov and select "Subscribe to e-mail alerts" under the "Order GAO Products" heading.

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. General Accounting Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Public Affairs

Jeff Nelligan, Managing Director, NelliganJ@gao.gov (202) 512-4800
U.S. General Accounting Office, 441 G Street NW, Room 7149
Washington, D.C. 20548

PRINTED ON RECYCLED PAPER

United States
General Accounting Office
Washington, D.C. 20548-0001

Official Business
Penalty for Private Use $300

Address Service Requested

Presorted Standard
Postage & Fees Paid
GAO
Permit No. GI00