September 2005

INFORMATION TECHNOLOGY

FBI Is Taking Steps to Develop an Enterprise Architecture, but Much Remains to Be Accomplished

GAO

Accountability ★ Integrity ★ Reliability

INFORMATION TECHNOLOGY

FBI Is Taking Steps to Develop an Enterprise Architecture, but Much Remains to Be Accomplished

Why GAO Did This Study

The Federal Bureau of Investigation (FBI) is currently modernizing its information technology (IT) systems to support its efforts to adopt a more bureauwide, integrated approach to performing its mission. A key element of such systems modernization programs is the use of an enterprise architecture (EA), which is a blueprint of an agency's current and planned operating and systems environment, as well as an IT investment plan for transitioning between the two. The conference report accompanying FBI's fiscal year 2005 appropriations directed GAO to determine (1) whether the FBI is managing its EA program in accordance with established best practices and (2) what approach the bureau is following to track and oversee its EA contractor, including the use of effective contractual controls.

What GAO Recommends

In light of its prior FBI EA program recommendations, GAO is making no additional recommendations relative to the adoption of architecture management best practices. However, GAO is making recommendations to ensure that effective contracting management practices are employed. In written comments on a draft of this report, the FBI stated that it appreciated GAO's assessment of its EA program and said that the bureau will continue to strive toward having a robust EA program supported by effective contract management practices.

www.gao.gov/cgi-bin/getrpt?GAO-05-363.

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

The FBI is managing its EA program in accordance with many best practices, but other such practices have yet to be adopted. These best practices, which are described in GAO's EA management maturity framework, are those necessary for an organization to have an effective architecture program. Examples of practices that the bureau has implemented include establishing a program office that is responsible for developing the architecture, having a written and approved policy governing architecture development, and continuing efforts to develop descriptions of the FBI's "as is" and "to be" environments and sequencing plan. The establishment of these and other practices represents important progress from the bureau's status 2 years ago, when GAO reported that the FBI lacked both an EA and the means to develop and enforce one. Notwithstanding this progress, much remains to be accomplished before the FBI will have an effective EA program. For example, the EA program office does not yet have adequate resources, and the architecture products needed to adequately describe either the current or the future architectural environments have not been completed. Until the bureau has a complete and enforceable EA, it remains at risk of developing systems that do not effectively and efficiently support mission operations and performance.

The FBI is relying heavily on contractor support to develop its EA; however, it has not employed effective contract management controls in doing so. Specifically, the bureau has not used performance-based contracting, an approach that is required by federal acquisition regulations whenever practicable. Further, the bureau is not employing the kind of effective contractor tracking and oversight practices specified in relevant acquisition management guidance. According to FBI officials, the agency's approach to managing its EA contractor is based on its long-standing approach to managing IT contractors: that is, working with the contractor on iterations of each deliverable until the bureau deems it acceptable. This approach, in GAO's view, is not effective and efficient. According to FBI officials, as soon as the bureau completes an ongoing effort to redefine its policies and procedures for managing IT programs (including, for example, the use of performance-based contracting methods and the tracking and oversight of contractor performance), it will adopt these new policies and procedures. Until effective contractor management policies and procedures are defined and implemented on the EA program, the likelihood of the FBI effectively and efficiently producing a complete and enforceable architecture is diminished.

Contents

Abbreviations

CIO	chief information officer
EA	enterprise architecture
FBI	Federal Bureau of Investigation
IT	information technology
OMB	Office of Management and Budget

United States Government Accountability Office
Washington, D.C. 20548

September 9, 2005

The Honorable Richard C. Shelby
Chairman
The Honorable Barbara A. Mikulski
Ranking Minority Member
Subcommittee on Commerce, Justice, and Science
Committee on Appropriations
United States Senate

The Honorable Frank R. Wolf
Chairman
The Honorable Alan B. Mollohan
Ranking Minority Member
Subcommittee on Science, State, Justice, and Commerce, and Related
Agencies
Committee on Appropriations
House of Representatives

The Honorable Judd Gregg
United States Senate

The Federal Bureau of Investigation (FBI) is attempting to replace much of
its 1980's-based information technology (IT) systems environment to better
support its plans for an integrated bureauwide approach to performing
critical mission operations, including terrorism prevention and federal
crime investigation. Our research and experience in reviewing federal
agency system modernization programs, including the FBI's, shows that
attempting such programs without a well-defined and enforceable
enterprise architecture (EA) results in nonintegrated, stand-alone systems
that are duplicative and do not effectively and efficiently support mission
performance.

In September 2003, we reported[1] that the FBI needed an EA to guide its
modernization activities and recommended that the FBI Director designate
the development of a complete architecture as a bureauwide priority and
manage the effort accordingly. In response, the FBI initiated efforts to
accomplish this goal, including hiring a contractor to assist the bureau in

---

[1]GAO, *Information Technology: FBI Needs an Enterprise Architecture to Guide Its
Modernization Activities*, GAO-03-959 (Washington, D.C.: Sept. 25, 2003).

this endeavor. Because of the importance of the EA to the FBI's modernization program, the conference report accompanying the fiscal year 2005 Consolidated Appropriations Act[2] directed us to determine (1) whether the FBI is managing its EA program in accordance with established best practices and (2) what approach the bureau is following to track and oversee its EA contractor, including the use of effective contractual controls. Details of our objectives, scope, and methodology are in appendix I.

Results in Brief

The FBI is managing its EA program in accordance with many best practices, but it has yet to adopt others. In our architecture management maturity framework,[3] we define practices that are associated with effective architecture programs. The bureau has implemented a number of these. For example, the bureau has established a program office that is responsible for the development of the architecture. In addition, the bureau has issued a written and approved policy governing architecture development. It also has ongoing efforts to develop and complete a target architecture, which describes an enterprise's future business, performance, information/data, application/service, and technology environments. This important progress has occurred since our September 2003 review (when we reported that the bureau lacked both an architecture and the means to develop and enforce one), in part, because FBI top management has demonstrated commitment to the EA program. Nonetheless, much remains to be accomplished before the EA program will be effective. For example, the architecture program office does not yet have adequate resources, the bureau's "as is" and "to be" architectures are not complete, and the bureau has not yet begun to develop its investment plans for transitioning from the "as is" to the "to be" states. Until the bureau has a complete and enforceable architecture, it remains at risk of developing systems that do not effectively and efficiently support mission operations and performance.

The FBI is relying heavily on contractor support to develop its EA, but it has not employed effective contract management controls in doing so. In

---

[2]*Making Appropriations for Foreign Operations, Export Financing, and Related Programs for the Fiscal Year Ending September 30, 2005, and for Other Purposes,* House of Representatives Report 108-792 (Nov. 20, 2004), Conference Report to accompany H.R. 4818, Consolidated Appropriations Act, 2005 (Pub. L. 108-447, Dec. 8, 2004).

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

particular, it has not used performance-based contracting, an approach that is required by federal acquisition regulations whenever practicable. Also, the bureau is not employing effective contractor tracking and oversight practices, as specified in relevant acquisition management guidance. More specifically, although the contract's statement of work defines when products are due (i.e., timeliness standards), it does not specify the products in results-oriented, measurable terms. Further, it does not specify quality standards for products and does not define incentives for addressing either timeliness or quality standards. Finally, the bureau has not developed a plan for assuring the quality of the work produced by the contractor. According to FBI officials, the bureau is managing its EA contractor as it has historically managed IT contractors: working with the contractor on iterations of each deliverable until it is acceptable. In our view, such an approach is neither effective nor efficient. Bureau officials stated that the Office of the Chief Information Officer (CIO) is currently developing standard IT management policies and procedures governing, among other things, the adoption of performance-based contracting methods and contractor tracking and oversight processes. However, officials could not provide a time frame for when this would occur. Until effective contractor management policies and procedures are defined and implemented on its architecture EA program, the likelihood of the FBI effectively and efficiently producing a complete and enforceable architecture is diminished.

We have previously made a comprehensive set of recommendations for strengthening the FBI's EA program, and so we are making no additional recommendations on this topic. In light of the FBI's heavy reliance on contractor assistance in developing its EA and the state of its contract management controls, we are making two recommendations with regard to use of performance-based contracting and tracking and oversight of contractor activities.

In written comments on a draft of this report, the FBI agreed that the bureau had made progress in developing its architecture. The FBI also stated that the bureau would continue to strive to develop a robust EA program supported by effective contracting management practices. The FBI noted its success using fixed-price contracts and stated that it intends to increase its use of performance-based contracting.
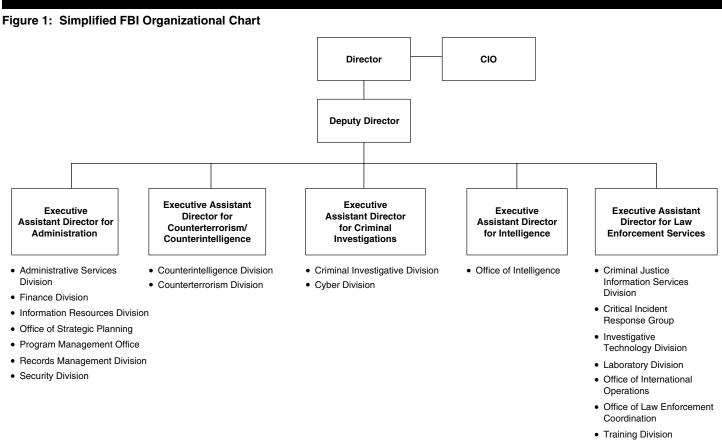
Background

The FBI was founded in 1908 to serve as the primary investigative unit of the Department of Justice. Its missions include protecting the nation from foreign intelligence and terrorist threats, investigating serious federal crimes, providing leadership and assistance to law enforcement agencies, and being responsive to the public in the performance of these duties. Approximately 12,000 special agents and 16,000 mission support personnel are located in the bureau's Washington, D.C., headquarters and in more than 450 offices in the United States and 45 offices in foreign countries.

Mission responsibilities at the bureau are divided among the following five major organizational components:

- *Counterterrorism and Counterintelligence:* identifies, assesses, investigates, and responds to national security threats.

- *Intelligence:* collects, analyzes, and disseminates information on evolving threats to the United States.

- *Criminal Investigations:* investigates serious federal crimes and probes federal statutory violations involving exploitation of the Internet and computer systems.

- *Law Enforcement Services:* provides law enforcement information and forensic services to federal, state, local, and international agencies.

- *Administration:* manages the bureau's personnel program, budgetary and financial services, records, information resources, and information security.

Each component is headed by an Executive Assistant Director who reports to the Deputy Director, who, in turn, reports to the Director. The components are further organized into 19 subcomponents, such as divisions, offices, and groups. Supporting these subcomponents are various staff offices, including the Office of the CIO. Figure 1 shows a simplified organizational chart of the components, subcomponents, Office of the CIO, and their respective reporting relationships.

Figure 1: Simplified FBI Organizational Chart

Source: GAO analysis of FBI data.

The Office of the CIO's responsibilities include preparing the bureau's IT strategic plan and operating budget; operating and maintaining existing systems and networks; developing and deploying new systems; defining and implementing IT management policies, procedures, and processes; and developing and maintaining the bureau's EA. To carry out these responsibilities, the Office of the CIO is organized into four subordinate offices. Figure 2 shows a simplified organizational chart of the CIO's office, subordinate offices, and their reporting relationships; a brief description of each office's responsibilities is in table 1. The FBI's EA program is in the CIO's Office of IT Policy and Planning.
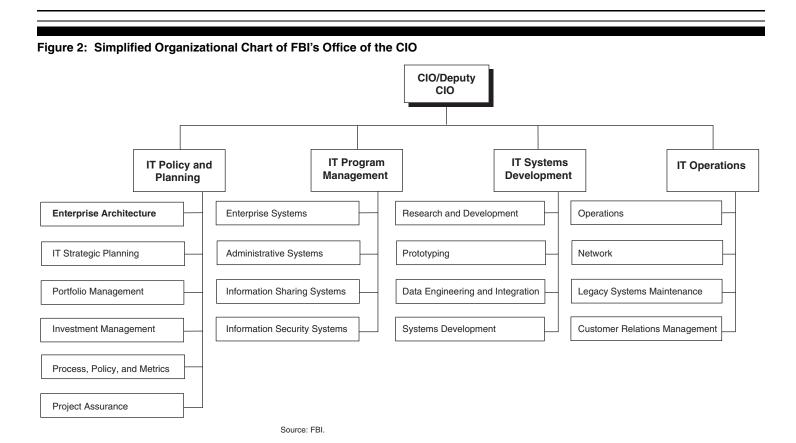
Figure 2: Simplified Organizational Chart of FBI's Office of the CIO

Source: FBI.

Table 1: Responsibilities of CIO Offices

Office	Responsibilities
Policy and Planning	Provides the resources, tools, and staff to define, coordinate, and oversee implementation of approved IT programs and projects. Responsible for IT investment management, strategic planning, portfolio management, EA, IT processes and policies, IT metrics, and project assurance, and for coordinating and facilitating all five of the enterprise IT boards.
Program Management	Provides the resources, tools, and staff to define and implement IT programs and projects. Also provides management and coordination between IT programs and projects. Responsible for ensuring that a program/project manager is assigned to each program or project.
Systems Development	Performs research and provides technical development and system engineering support for new IT systems and, as required, selected existing systems, including the network and legacy systems. Responsible for assigning a Systems Development Manager for each program or project.
Operations and Maintenance Organization	Provides the resources, tools, and staff to operate and maintain existing systems and to provide customer support service for those systems. Helps in the transition of new systems into the production environment.

Source: FBI.

To execute its mission responsibilities, the FBI has historically relied extensively on IT. For example, it relies on such computerized IT systems as the Combined DNA[4] Index System to support forensic examinations and the National Crime Information Center and the Integrated Automated Fingerprint Identification System to help state and local law enforcement agencies identify criminals. The FBI reports that it collectively manages hundreds of systems, networks, databases, applications, and associated IT tools. As we previously reported,[5] the FBI's IT environment includes outdated, nonintegrated systems that do not optimally support mission operations.

Following the terrorist attacks of September 11, 2001, the FBI was forced to rethink its mission. As we have reported,[6] this resulted in the bureau shifting its mission focus to detecting and preventing possible future attacks and ultimately led to the FBI's commitment to reorganize and

---

[4]Deoxyribonucleic acid.

[5]GAO-03-959.

[6]For example, see GAO, *FBI Transformation: FBI Continues to Make Progress in Its Efforts to Transform and Address Priorities*, GAO-04-578T (Washington, D.C.: Mar. 23, 2004).

transform itself. According to the bureau, the complexity of this mission shift, along with the changing law enforcement environment, has strained its existing patchwork of IT systems, which were developed and deployed on an ad hoc basis. The bureau reports that these circumstances will require a major overhaul in its IT systems environment.

To effect this change, the FBI has undertaken an organizational transformation and systems modernization effort. Major goals of the transformation are, among other things, to develop the capability to become a proactive rather than a reactive organization, embrace intelligence as a professional and operational competency, and leverage information across the bureau and with other agencies to "connect the dots."According to the FBI, an integral part of the transformation will be modernizing the IT systems that support the bureau's processes. The FBI reports that it will spend approximately $390 million on modernization projects in fiscal year 2005 out of a total IT budget of $737 million. To guide and constrain these and future system modernization investments, the FBI has initiated an effort to align its investments with the new mission being implemented via its transformation. The FBI has stated that a foundational element of this effort is a bureauwide EA.

An EA Is Critical to Successful Systems Modernization

Effective use of EAs, or modernization blueprints, is a trademark of successful public and private organizations. For more than a decade, we have promoted the use of architectures to guide and constrain system modernizations, recognizing them as a crucial means to a challenging goal: agency operational structures that are optimally defined in both business and technological environments. The Congress, the Office of Management and Budget (OMB), and the federal CIO Council have also recognized the importance of an architecture-centric approach to modernization. The Clinger-Cohen Act of 1996[7] mandates that agency CIOs develop, maintain, and facilitate the implementation of an IT architecture. Further, the E-Government Act of 2002[8] requires OMB to oversee EA development within and across agencies.

An EA is a systematically derived snapshot—in useful models, diagrams, and narrative—of a given entity's operations (business and systems),

---

[7]The Clinger-Cohen Act of 1996, 40 U.S.C. sections 11312 and 11315(b)(2).

[8]E-Government Act of 2002 (Pub. L. 107-347, Dec. 17, 2002).

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 both for 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. In doing so, EAs link organizations' strategic plans with program implementations.

Among others, OMB, the National Institute of Standards and Technology, and the federal CIO Council have issued frameworks that define the scope and content of architectures. [9] In addition, OMB has since issued a collection of five reference models[10] (Business, Performance, Data/Information, Service, and Technical) that are intended to facilitate governmentwide improvement through cross-agency analysis and the identification of duplicative investments, gaps, and opportunities. While these various frameworks differ in their nomenclatures and modeling approaches, they consistently provide for defining an architecture's operations in both logical and technical terms and providing these perspectives for both the "as is" and the "to be" environments, as well as the investment roadmap.

Managed properly, an EA can clarify and help to optimize the interdependencies and relationships among an organization's business

---

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

[10]The *Business Reference Model* is intended to describe the business operations of the federal government independent of the agencies that perform them, including defining the services provided to state and local governments. The *Performance Reference Model* is to provide a common set of general performance outputs and measures for agencies to use to achieve business goals and objectives. The *Data and Information Reference Model* is to describe, at an aggregate level, the type of data and information that support program and business line operations, and the relationships among these types. The *Service Component Reference Model* is to identify and classify IT service (i.e., application) components that support federal agencies and promote the reuse of components across agencies. The *Technical Reference Model* is to describe how technology is supporting the delivery of service components, including relevant standards for implementing the technology.

operations and the underlying IT infrastructure and applications that support these operations. Employed in concert with other important management controls, such as portfolio-based capital planning and investment control practices, architectures can greatly increase the chances that an organization's operational and IT environments will be configured to optimize its mission performance. Our experience with federal agencies has shown that making IT investments without defining these investments in the context of an architecture often results in systems that are duplicative, not well integrated, and unnecessarily costly to maintain and interface.[11]

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

According to guidance published by the federal CIO Council, effective architecture management consists of a number of key practices and conditions.[12] In April 2003, we published a maturity framework that arranges key best practices and conditions of the federal CIO Council's guide into five hierarchical stages, with Stage 1 representing the least mature and Stage 5 being the most mature.[13] 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, and the stages and their core elements are shown in table 2. (See app. II for a more detailed description of our framework and associated core elements.)

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

---

[11]See, for example, GAO, *Homeland Security: Efforts Under Way to Develop Enterprise Architecture, but Much Work Remains*, GAO-04-777 (Washington, D.C.: Aug. 6, 2004); *DOD Business Systems Modernization: Limited Progress in Development of Business Enterprise Architecture and Oversight of Information Technology Investments*, GAO-04-731R (Washington, D.C.: May 17, 2004); *Information Technology: Architecture Needed to Guide NASA's Financial Management Modernization*, GAO-04-43 (Washington, D.C.: Nov. 21, 2003); *DOD Business Systems Modernization: Important Progress Made to Develop Business Enterprise Architecture, but Much Work Remains*, GAO-03-1018 (Washington, D.C.: Sept. 19, 2003); and *Information Technology: DLA Should Strengthen Business Systems Modernization Architecture and Investment Activities*, GAO-01-631 (Washington, D.C.: June 29, 2001).

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

[13]GAO-03-584G.

Stage 1 agencies may have initiated some architecture activity, these agencies' efforts are ad hoc and unstructured, lack institutional leadership and direction, and do not provide the management foundation necessary for successful architecture development.

2. *Building the EA management foundation.* The organization recognizes that the architecture is a corporate asset by vesting accountability for it in an executive body that represents the entire enterprise. At this stage, an organization assigns architecture management roles and responsibilities and establishes plans for developing architecture 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 architecture products. The scope of the architecture has been defined to encompass the entire enterprise, whether organization based or function based.

4. *Completing the EA.* The organization has completed its architecture products—meaning that the products have been approved by the architecture 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 architecture products. Additionally, evolution of the approved products is governed by a written architecture 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 architecture 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 architecture benefits or return on investment, and adjustments are continuously made to both the architecture management process and the architecture products.

Table 2: GAO's EA Management Framework (Version 1.1)

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 automated tool.
	EA plans call for describing the "as is" and "to be" environments, and a sequencing plan.
	EA plans call for describing the enterprise in terms of business, performance, information/data, application/service, and technology.
	EA plans call for business, performance, information/data, application/service, and technology descriptions to address security.
	EA plans call for developing metrics for measuring EA progress, quality, compliance, and return on investment.
Stage 3: Developing EA products[a]	Written and approved organization policy exists for EA development.
	EA products are under configuration management.
	EA products describe or will describe the enterprise's business, performance, information/data, application/service, and the technology that supports them.
	EA products describe or will describe the "as is" and the "to be" environments, and a sequencing plan.
	Business, performance, information/data, application/service, and technology descriptions address or will address security.
	Progress against EA plans is measured and reported.
Stage 4: Completing EA products[a]	Written and approved organization policy exists for EA maintenance.
	EA products and management processes undergo independent verification and validation.
	EA products describe the enterprise's business, performance, information/data, application/service, and the technology that supports them.
	EA products describe the "as is" and the "to be" environments, and a transitioning plan.
	Business, performance, information/data, application/service, and technology descriptions address security.
	Organization's chief information officer has approved current version of 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 to manage change[a]	Written and 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.

Stage	Core elements
	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.

[a]Includes all elements from previous stages.

Our Prior Reviews Have Emphasized the Need for the FBI to Establish Architecture Management Capabilities

Over the past several years, reviews of the FBI's efforts to leverage IT to support its transformation have identified the bureau's lack of an EA as a significant management weakness. For example, during 2002, we reported[14] that the FBI did not have an EA. Because our research and experience at federal agencies shows that architectures are an essential ingredient to success for transformations like the FBI's, we reported that the bureau should establish the management foundation that is necessary to begin successfully developing, implementing, and maintaining an EA.

Between September 2003 and September 2004, we reported[15] on a number of FBI IT transformation challenges, including effectively developing and using an architecture. More specifically, we reported[16] in September 2003 that the bureau had not yet acted on our recommendation for an EA, having only established 1 of the 31 key EA management capabilities described in our architecture management maturity framework, and that this limited capability was due in part to the fact that the architecture's development was not being treated as an agency priority. Accordingly, we recommended that the Director make architecture development and use a priority, and we provided additional recommendations to help the bureau establish the management capabilities needed to develop, implement, and maintain its architecture. The FBI agreed with our recommendations.

---

[14]For example, see GAO, *FBI Reorganization: Initial Steps Encouraging but Broad Transformation Needed*, GAO-02-865T (Washington, D.C.: June 21, 2002).

[15]GAO-03-959; GAO, *Federal Bureau of Investigation's Comments on Recent GAO Report on Its Enterprise Architecture Efforts*, GAO-04-190R (Washington, D.C.: Nov. 14, 2003); and *Foundational Steps Being Taken to Make Needed FBI Systems Modernization Management Improvements*, GAO-04-842 (Washington, D.C.: Sept. 10, 2004).

[16]GAO-03-959.

Since we reported on the FBI's lack of an architecture, others have similarly reported on this gap in the bureau's ability to effectively modernize its systems and transform its operations. For example, in March 2004, the Department of Justice Inspector General testified[17] that the lack of an architecture was a contributing factor to the continuing cost and schedule shortfalls being experienced by the bureau on its Trilogy investigative case management system, which was the FBI's centerpiece systems modernization project. Moreover, the National Research Council reported[18] in May 2004 that while the bureau had made significant progress in its IT systems modernization program, the FBI was not on the path to success, in part, because it had not yet developed an EA.

The FBI initiated its current effort to develop an architecture in late 2003. For example, in March 2004, the bureau awarded a $1.2 million firm, fixed-price contract for assistance in developing, maintaining, and implementing an EA. It subsequently awarded the same contractor two fixed-price contracts to provide EA security and integration services.[19] Although these contracts are supporting the Office of the CIO, responsibility for contract management resides with the Office of the Chief Financial Officer.

FBI Has Implemented Some Important EA Management Practices, but It Has Yet to Implement Others

As we previously reported,[20] it is critical that the FBI have and use a well-defined EA to guide and constrain its IT investment decisions. We recommended that in order to effectively develop and implement an architecture, the bureau employ rigorous and disciplined architecture management practices. Such practices form the basis of our architecture management maturity framework. The bureau has thus far implemented most of our framework's key practices associated with establishing an architecture management foundation, but important foundational practices

---

[17]U.S. Department of Justice, Office of the Inspector General, *Statement of Glenn A. Fine, Inspector General, before the Senate Committee on Appropriations, Subcommittee on Commerce, Justice, State, and the Judiciary* (Washington, D.C.: Mar. 23, 2004).

[18]National Research Council, *A Review of FBI's Trilogy Information Technology Modernization Program* (Washington, D.C.: May 10, 2004).

[19]The first, at a cost of $414,000, is to provide technical services to the program office team developing the security view of the architecture. The second, at a cost of $416,000, is to provide two contractor staff to, among other things, support a program office group tasked with integrating various EA products.

[20]GAO-03-959.

are still missing. It has also implemented key practices related to developing the architecture; however, most architecture development practices are not yet fully implemented, and virtually all practices that are key to completing and leveraging the architecture for organizational change remain to be implemented. While the bureau's EA efforts to date represent important progress from where it was in 2003, when we last assessed its efforts, much remains to be accomplished before the FBI will have an effective EA program. Without such a program, the bureau will be challenged in its efforts to effectively and efficiently modernize its systems in a way that minimizes duplication and overlap, maximizes integration, and effectively supports organizational transformation.

In March 2005, the FBI completed an EA baseline report on the status of its "as is" EA activities.[21] The purpose of the report was to, among other things, provide a "high-level snapshot" of where it stood in determining and understanding current bureau business processes and supporting IT structures and systems and how it was managing its ongoing architecture development efforts. In May 2005, the bureau issued a similar report on its "to be" architecture activities.[22] On the basis of these reports, along with other documentation and officials' statements, we determined that the bureau has satisfied 15 of the 31 core elements specified in our architecture management maturity framework, including 7 Stage 2 elements, all Stage 3 elements, 1 Stage 4 element, and 1 Stage 5 element (see table 3). For the remaining elements, the bureau has efforts planned and under way that are intended to satisfy them.

[21]U.S. Department of Justice, Federal Bureau of Investigation, *Enterprise Architecture Integrated Baseline Architecture Report*, Version 2.0 (Redacted) (Mar. 4, 2005).

[22]U.S. Department of Justice, Federal Bureau of Investigation, *Enterprise Architecture Target Architecture Report*, Version 1.0 (May 31, 2005).

Table 3: Summary of the FBI's Satisfaction of Key Architecture Management Practices Described in GAO EA Management Maturity Framework (Version 1.1)

Stage	Core elements	Status as of April 2005
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 automated tool.	—
	EA plans call for describing the "as is" and "to be" environments and a sequencing plan.	✓
	EA plans call for describing the enterprise in terms of business, performance, information/data, application/service, and technology.	✓
	EA plans call for business, performance, information/data, application/service, and technology descriptions to address security.	✓
	EA plans call for developing metrics for measuring EA progress, quality, compliance, and return on investment.	✓
Stage 3: Developing EA products[a]	Written and approved organization policy exists for EA development.	✓
	EA products are under configuration management.	✓
	EA products describe or will describe the enterprise's business, performance, information/data, application/service, and the technology that supports them.	✓
	EA products describe or will describe the "as is" and the "to be" environments, and a sequencing plan.	✓
	Business, performance, information/data, application/service, and technology address or will address security.	✓
	Progress against EA plans is measured and reported.	✓
Stage 4: Completing EA products[a]	Written and approved organization policy exists for EA maintenance.	—
	EA products and management processes undergo independent verification and validation.	✓
	EA products describe the enterprise's business, performance, information/data, application/service, and the technology that supports them.	—
	EA products describe the "as is" and the "to be" environments, and a transitioning plan.	—
	Business, performance, data, application, and technology descriptions address security.	—
	Organization's chief information officer has approved current version of EA.	—
	Committee or group representing the enterprise or the investment review board has approved current version of EA.	—

Stage	Core elements	Status as of April 2005
	Quality of EA products is measured and reported.	—
Stage 5: Leveraging the EA to manage change[a]	Written and 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.	—

✓ Fully satisfied

— Not fully satisfied

Source: GAO based on FBI data.

Note: Shading indicates that satisfaction of element has occurred since our September 2003 assessment.

[a]To achieve a particular stage includes satisfying the specified elements in the stage plus all elements from previous stages. For example, to achieve Stage 3 requires achieving the stage-specific elements plus those in Stages 1 and 2.

More specifically, for Stage 2, the bureau has satisfied seven of nine core elements. For example, in early 2004, the bureau established a program office—located in the CIO's office and headed by a senior level executive—that is responsible for EA development and maintenance, including drafting and executing a program management plan. This program office includes a chief architect and five key senior level architect positions for business, applications, information, technology, and security. The office also has positions that are to perform support functions such as quality assurance, risk management, and configuration control.[23]

The bureau also established an Enterprise Architecture Board that includes senior representation from across all bureau business areas and has assigned the board responsibility for directing, overseeing, and approving the architecture. Minutes of board meetings show that this organization meets about every 2 weeks to oversee EA program progress, provide executive direction, and review and approve EA plans and products. These minutes also show that CIO officials and business area representatives regularly attend the meetings.

---

[23]According to the FBI, the program office has 13 positions in total.

In addition, the bureau has developed a number of plans, including a program management plan (dated October 2004). According to these plans, the architecture is to describe the "as is" and "to be" environments, as well as a sequencing plan. Moreover, the plans call for describing the enterprise in terms of business, performance, data, application, and technology. These plans also include a schedule of tasks to be performed, associated milestones, and an estimate of resources (e.g., funding, staffing, contractor assistance) for fiscal years 2004 through 2007. In addition, these plans call for developing performance metrics to measure EA development and execution and provide for establishing management controls, such as risk management, quality assurance, and configuration control, for developing and maintaining the architecture.

Other Stage 2 core elements have yet to be fully addressed. For example, the EA program office does not yet have adequate resources. According to the framework, an organization should have the resources (e.g., funding, human capital) to establish and effectively manage its architecture. According to FBI officials, they have adequate financial resources to fund the program and sufficient contractor assistance, and they have been able to use bureau and contractor personnel to staff most of the 13 program office staff positions. However, core staff positions identified by the bureau have not yet been filled: four of the five key architect positions mentioned earlier are vacant. Bureau officials told us that job announcements have been issued for the four key architect positions, but it has been a challenge finding the right candidates. According to the FBI, failing to have these key staff on board hampers the program office's ability to perform planned tasks. Having qualified staff serving as the core team is important because without them, the program office does not have the proper knowledge, skills, and abilities to properly execute the EA program, including managing and overseeing its contractors.

In addition, although the FBI has selected a framework[24] to determine the type of architecture products to be developed and has acquired an automated tool[25] to capture the content of its products, the bureau does not have a defined methodology (i.e., the specific steps and methods)

---

[24]The FBI initially established plans to use the Federal Enterprise Architecture Framework and later switched over to the five Federal Enterprise Architecture Reference Models recommended by OMB.

[25]The tool being used by the bureau is Popkin System Architect. It serves as a repository for EA products and other related documents.

documenting how it will develop the products' content. As stated in our framework, a methodology is important because it defines (and thus permits stakeholders and others to understand) the steps necessary to perform the activities associated with capturing EA content in a coherent, consistent, accountable, and repeatable manner. For this reason, our architecture maturity framework calls for using a methodology in conjunction with an EA framework and automated tool. Collectively, these permit architecture development to occur in an effective and efficient manner.

Instead of a defined methodology, the bureau is relying on a combination of its chief architect's knowledge and certain documentation, such as an EA alignment plan that describes, among other things, the products to be developed, the order in which they are to be developed, the relationships among products, and analyses that are to be performed to help identify gaps and redundancies in the contents of these products. However, this documentation does not include either the specific steps or methods that explain how the content of products is to be developed and documented. It is important to have a documented methodology that is available to and understood by those engaged in providing EA product content, because without one, there is increased risk that products will be inconsistent, incomplete, and incorrect, and thus require rework.

For Stage 3, the bureau has satisfied all six core elements. In particular, the bureau issued a policy in August 2003 that defines, among other things, the scope of the architecture and identifies the major stakeholders, including their roles and responsibilities.

In addition, the bureau has developed a configuration management plan that defines management structures and processes for identifying, tracking, monitoring, reporting, and auditing changes to the architecture products. The plan establishes a configuration control board and makes the security architect responsible for initiating board meetings and ensuring that audits are conducted as intended. To date, this board has identified and begun tracking such changes. For example, products, including the program management plan, EA principles, "as is" architecture, and EA software tool, have been identified and placed under configuration management in accordance with the plan.

Further, the program office reports that it is in the process of developing its "as is" architecture. According to the March 2005 report, the bureau has issued several iterations of a "high-level" version of its "as is" architecture

that describes the bureau's business, data, application, and technology environments. However, these iterations do not include performance descriptions. Moreover, the other "as is" descriptions are not complete, according to the report. For example, as part of the information/data description, the program office is in the process of completing ongoing efforts to map FBI data to the business processes that use these data. In addition, as part of the application description, the program office is working to develop a system architecture diagram to show how the various IT applications currently interrelate. Also, while the program office has developed a business architecture description, it has not performed a detailed decomposition of the business processes described. The bureau had planned to complete the remaining work on the "as is" architecture by mid-summer.

The office also is in the process of developing the "to be" architecture. According to the FBI's May 2005 report, the initial version of the "to be" architecture includes business, performance, information/data, service, and technology descriptions. However, the report identifies additional work needed to complete this version. For example, according to the report, the service reference models need to be further defined to provide a detailed framework that supports the transition to the "to be" environment. In addition, the bureau reports that data exchange models need to be developed to provide better understanding of data exchange processes and whether opportunities exist for improvement. Further, the bureau reports that it needs to develop a framework so that it can better understand the relationships among EA components, such as between the business reference model and the service reference model, and between the service reference model and the technology reference model. The bureau plans to issue the next version of its "to be" architecture in fiscal year 2006.

In addition, the bureau reports it has developed a "high level" description of a sequencing plan that is not yet complete; the next version of the plan is scheduled for issuance in September 2005.

Two additional elements (one Stage 4 and one Stage 5 element) have also been satisfied. Specifically, while EA products and processes to date have not been independently verified and validated, the FBI hired a contractor in April 2005 to begin performing such assessments on both the EA products and the processes used to develop them. According to the contract statement of work, the results of these assessments are to be shared with the program office and reported to the steering committee.

Also, the bureau has defined a management structure and process to formally manage EA change. According to its configuration management plan (dated February 3, 2005), the bureau is using an automated tool to manage critical EA work products as they are developed and changed. Further, the bureau established a Change Management Board to resolve critical issues, including those that require a major commitment of resources, vary from the EA strategy, or require a policy change.

Beyond these two elements, 14 core elements in Stages 4 and 5 have yet to be satisfied. In particular, key architecture products have yet to be completed. As previously noted, the bureau is still in the process of developing both its "as is" and "to be" architectures, for example. The sequencing plan is also a work in process. (A summary of the results of our assessment on the FBI's satisfaction of the core elements for each of the stages are provided in app. III.)

Discussing the bureau's EA program, the FBI's CIO said that significant progress has been made, which he attributed to top-level organizational commitment and focus on EA, as well as assignment of bureauwide IT budget control and authority to the CIO. Despite this progress, much remains to be accomplished before the FBI will have an effective EA program. According to our framework, effective architecture management is generally not achieved until an enterprise has a completed and approved architecture that is being effectively maintained and is being used to leverage organizational change and support investment decision making; having these characteristics is equivalent to having satisfied all of the Stage 2 and 3 core elements and many of the Stage 4 and 5 elements.

Until the bureau gets to that stage, it will be challenged in its efforts to implement modernized systems in a way that minimizes overlap and duplication and maximizes integration and mission support. Our prior reviews of federal agencies and research of architecture best practices have shown that attempting to modernize systems without a well-defined and verifiable architecture and associated management capabilities 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.

Bureau Is Not Effectively Managing Its EA Contractor

Federal acquisition regulations and relevant IT acquisition management guidance recognize the importance of effectively managing contractor activities. The Federal Acquisition Regulation (FAR), for example, directs agencies to use performance-based contracting to the maximum extent practicable when acquiring most services.[26] Under the FAR, performance-based contracting includes (1) defining the work to be performed in measurable, results-oriented terms; (2) specifying performance standards (quality and timeliness) that are tied to contractual requirements; (3) having a quality assurance plan that describes how the contractor's performance in meeting requirements will be measured against standards; and (4) establishing positive and negative contractor performance incentives. The FAR and associated regulations[27] also require government oversight of contracts to ensure that the contractor (the service provider) performs the requirements of the contract, and the government (the service receiver or customer) receives the service as intended. However, the regulations do not prescribe specific methods for this oversight.

Other acquisition management guidance[28] identifies effective contractor tracking and oversight as a key activity and describes a number of practices associated with this activity, including

- establishing a written policy for contract tracking and oversight,

- designating responsibility for contract tracking and oversight activities,

- establishing a group that is responsible for managing contract tracking and oversight activities, and

- using approved contractor planning documents as a basis for tracking and overseeing the contractor.

The FBI's approach to managing its EA contract does not include most of the performance-based contracting features described in the FAR. Specifically, although the contract's statement of work defines when

---

[26]See Federal Acquisition Regulation, section 37.102(a).

[27]See Federal Acquisition Regulations Part 46, "Quality Assurance."

[28]See, for example, Carnegie Mellon Software Engineering Institute, *Software Acquisition Capability Maturity Model*, CMU/SEI-99-TR-002 (April 1999).

products are due (i.e., timeliness standards), it does not specify the products in results-oriented, measurable terms. For example, the statement of work defines requirements in terms of general product descriptions such as "as is" and "to be" architectures and a sequencing plan. Further, it does not specify quality standards for products and does not define incentives for addressing either timeliness or quality standards.

The bureau also does not have plans for assuring the quality of the contractor's work. Instead, bureau officials told us that they follow the bureau's long-standing approach of working with the contractor to determine whether each deliverable is acceptable. As an example, the bureau received a draft of its "as is" architecture on August 22, 2004. According to bureau officials, the draft was of poor quality, and the bureau did not accept it. The bureau then worked with the contractor to improve the quality of the product, and after several iterations, the bureau accepted a draft of the "as is" architecture on September 30, 2004. However, because the bureau did not have either quality standards or a quality assurance plan, the basis for acceptance was not available for us to independently assess.

In tracking and overseeing its contractor, the FBI also has not employed the kind of effective practices specified in relevant acquisition management guidance. For example, the bureau does not have a written policy to govern its tracking and oversight activities, has not designated responsibility or established a group for performing contract tracking and oversight activities, and has not developed an approved contractor monitoring plan. Instead, the bureau holds weekly status meetings with its EA contractor to discuss progress and plans, and it is receiving incremental drafts of work products in an effort to increase visibility into contractor activities and thereby minimize the number of unacceptable deliverables and associated rework.

FBI officials from the offices of the Chief Financial Officer and CIO attributed the current contract management approach to several factors. First, they said that the FBI has historically been challenged in developing statements of work that clearly define requirements and establish performance (quality and timeliness) standards, which are essential to effective performance-based contracting. Second, these officials stated that they are still working to define effective contract management controls. Specifically, as part of the CIO office's transformation, including implementing its recently assigned agencywide authority and control over IT resources, these officials are developing standard policies and procedures for managing IT. In particular, these policies and procedures

are to include an FBI-wide standard life-cycle management directive that is to define procedures for the use of performance-based contracting methods and the establishment of tracking and oversight structures, policies, and processes. The officials told us they began implementing parts of the directive in late June 2005, but added that certain key practices, such as acquisition management, were early drafts and required further development. However, the officials were unable to provide a date for when the drafts would be finalized and implementation of the practices would begin.

In the absence of performance-based contracting and effective tracking and oversight, the bureau's ability to effectively manage its EA contractor is constrained. This means that the FBI is at risk of taking more time and spending more money than necessary to produce a well-defined architecture.

Conclusions

Having a well-defined and enforced architecture is critical to the FBI's ability to effectively and efficiently modernize its mission operations and supporting IT environment. The bureau has taken steps aimed at developing such an architecture and has made important progress in doing so; however, much remains to be accomplished before it will have implemented our prior recommendations and established an effective EA program. As it moves forward, it is important for the bureau to employ all the effective architecture management practices that we have previously recommended, and to do so expeditiously. Moreover, given that the FBI's program is heavily relying on contractor support, it is also important for the bureau to ensure that it employs effective contract management controls that will enable it to, among other things, define contractor work to be performed in measurable, results-oriented terms; establish positive and negative contractor performance incentives; and define and implement contractor tracking and oversight processes consistent with acquisition management guidance. Currently, the FBI does not have such controls in place, and as a result, it is increasing the risk that it will take more time and money to develop a well-defined EA than is necessary. If the bureau does not begin employing the kind of effective contract management controls contained in federal regulations and related guidance, its architecture efforts will continue to be at risk. In turn, its systems modernization will continue to be challenged in its ability to efficiently and effectively support mission operations through modern IT systems.

Recommendations for Executive Action

In light of our prior comprehensive set of recommendations for strengthening the FBI's EA program, we are not making additional recommendations at this time relative to satisfying the practices embodied in our architecture management maturity framework.

Given the FBI's heavy reliance on contractor assistance in developing its EA and the state of its contract management controls, we recommend that the FBI Director direct the Chief Financial Officer, in conjunction with the CIO, to ensure that to the maximum extent practicable, performance-based contracting activities, along with effective contract tracking and oversight practices, are employed prospectively on all EA contract actions. This should include, among other things, defining contractor work in measurable, results-oriented terms; establishing positive and negative contractor performance incentives; and defining and implementing contractor tracking and oversight processes consistent with acquisition management guidance.

Agency Comments and Our Evaluation

In written comments on a draft of this report, signed by the CIO and reprinted in appendix IV, the FBI agreed that the bureau had made progress in developing its architecture. The FBI also stated that it appreciated our assessment and feedback on its EA program and that the bureau would continue to strive to develop a robust EA program supported by effective contract management practices. In this regard, the FBI cited steps under way to strengthen its EA management foundation. The FBI also noted our recommendation regarding the use of performance-based contracting, stating that its use of fixed-price contracting for EA support has been successful. We believe the FBI can benefit from increased use of performance-based contracting techniques even under firm, fixed-priced contracts. In this regard, the FBI agreed, stating that our recommendations provide for effective EA contract management practices and that it is now taking steps to increase its use of performance-based contracting. The FBI stated that it is in the process of increasing employee awareness and providing training on the performance-based approach.

We are sending copies of this report to the Chairmen and Ranking Minority Members of the Senate and House Appropriations Committees. We are also sending copies to the Attorney General; the Director, FBI; the Director, OMB; and other interested parties. This report will also be available at no charge on our 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 hiter@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO contacts and staff who made major contributions to this report are listed in appendix V.

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

Objectives, Scope, and Methodology

As specified in the conference report[1] accompanying the Consolidated Appropriations Act, 2005,[2] our objectives were to determine (1) whether the Federal Bureau of Investigation (FBI) is managing its enterprise architecture (EA) program in accordance with established best practices and (2) what approach the bureau is following to track and oversee its EA contractor, including the use of effective contractual controls.

For the first objective, we reviewed our EA management maturity framework, Version 1.1,[3] which organizes architecture management best practices into five stages of maturity. This framework is based on *A Practical Guide to Federal Enterprise Architecture*, published by the federal Chief Information Officer (CIO) Council.[4] We compared our framework with the ongoing efforts of the FBI's EA program. Specifically, we analyzed the bureau's EA plans and products, including program management and other plans, key architecture principles, work breakdown structures and corresponding milestones, Enterprise Architecture Board charters and meeting minutes, repository strategy, and EA status reports. We also analyzed relevant policies and procedures, including the bureau's EA Policy and the Information Technology Life Cycle Management Directive. Moreover, we reviewed draft architecture work products, including iterations of the "as is" and "to be" architectures; we did not, however, assess the contents or quality of these architectural work products because they were in varying degrees of completion and subject to ongoing change. Next, we compared our analyses with the EA management maturity framework practices to determine the extent to which the FBI was employing such effective management practices. We also interviewed bureau officials, such as the CIO, the chief architect, and the head of the EA program office.

---

[1]*Making Appropriations for Foreign Operations, Export Financing, and Related Programs for the Fiscal Year Ending September 30, 2005, and for Other Purposes*, House of Representatives Report 108-792 (Nov. 20, 2004), Conference Report to accompany H.R. 4818, Consolidated Appropriations Act, 2005 (Pub. L. 108-447, Dec. 8, 2004).

[2]Pub. L. 108-447 (Dec. 8, 2004).

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

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

For the second objective, we first reviewed key federal regulations and best practices and guidance. In particular, we reviewed relevant federal acquisition regulations on effective contract management, including performance-based contracting methods. Additionally, we reviewed the Software Engineering Institute's Software Acquisition Capability Maturity Model, version 1.02, for key contractor tracking and oversight best practices. We then analyzed EA contract documentation, including task orders, statements of work, and contract modifications. We also interviewed FBI officials, including the contracting office's technical representative for overseeing the EA contractor, the chief architect, and the head of the EA program office. We interviewed these officials to verify and clarify our understanding of the bureau's architecture contract management procedures and to determine whether the bureau is employing effective contractual controls. Additionally, we discussed with these officials the cause and impact of the current state of the bureau's contract management activities and policies.

We performed our work at FBI headquarters in Washington, D.C., from September 2004 to July 2005, in accordance with generally accepted government auditing standards.

Detailed Descriptions of Elements in GAO's EA Management Maturity Framework

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. The five stages and their associated core elements are described below.

At Stage 1, organizations are becoming aware of the value of an EA, but have not yet established the management foundation needed to develop one. Stage 1 has no core elements: by default, an organization that does not satisfy Stage 2 core elements is at Stage 1.

For Stage 2, our framework specifies nine key practices or core elements that are necessary to provide the management foundation for successfully launching and sustaining an architecture effort:

- *Ensure that adequate resources exist.* An organization should have the resources (funding, people, tools, and technology) to establish and effectively manage its architecture. This includes identifying and securing adequate funding to support EA activities; hiring and retaining the right people with the proper knowledge, skills, and abilities to plan and execute the EA program; and selecting and acquiring the right tools and technology to support EA activities.

- *Establish a committee or group representing the enterprise that is 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.

- *Establish a program office that is responsible for EA development and maintenance.* This organizational unit should be devoted to the EA program and responsible for developing a management plan and executing the plan. The plan should include a detailed work breakdown structure; resource estimates (e.g., funding, staffing, and training);

performance measures; and management controls for developing and maintaining the architecture.

- *Appoint a chief architect.* The chief architect should be responsible and accountable for the EA, supported by the architecture program office, and overseen by the architecture steering committee. The chief architect (in collaboration with the CIO, the architecture steering committee, and the organizational head) is instrumental in obtaining organizational buy-in for the architecture, 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 a framework, methodology, and automated tool to develop the architecture.* 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 architecture 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 architecture development and maintenance as a formal program.

- *Ensure that EA plans call for describing both the "as is" and "to be" environments in terms of business, performance, information/data, application/service, and technology.* An organization's program management plan should provide for defining and normalizing the current and future architectures in terms relevant to stakeholders from varying organization levels and disciplines.

- *Ensure that EA plans address security at each layer.* Plans should define how the organization will address security as a distinct area of operational and technology emphasis within the context of each layer.

- *Ensure that EA plans call for developing metrics for measuring EA progress, quality, compliance, and return on investment.* Plans should provide for developing metrics and should describe how these will be

used to measure (1) progress towards EA goals, (2) the quality of architecture products and management processes, (3) compliance with the architecture, and (4) EA return on investment.

At Stage 3, our framework specifies six core elements that are necessary to focus on architecture development activities:

- *Issue a written and approved organization policy for EA development.* A policy defines the scope of the architecture, including the requirement for a description of the current and target architectures, as well as an investment road map or sequencing plan specifying the move between the two.

- *Ensure that EA products are under configuration management.* This involves ensuring that changes to products are identified, tracked, monitored, documented, reported, and audited.

- *Ensure that EA products describe or will describe both the "as is" and the "to be" environments, as well as a sequencing plan.* Consistent with the EA program plans discussed in Stage 2, an organization should ensure that the EA products being developed are enterprisewide in scope and describe both the current and future environments, as well as a sequencing plan for moving from the current to the target environment.

- *Ensure that EA plans are described or will be described for both environments in terms of business, performance, information/data, application/service, and technology.* Products being developed or drafted should begin to address each of the given terms of reference, or include placeholders for later defining the enterprise in these terms.

- *Ensure that business, performance, information/data, application/service, and technology descriptions address or will address security.* This involves ensuring that each EA product (including those describing the "as is" and "to be" environments in terms of business, performance, information/data, application/service, and technology) explicitly describe how enterprise security is being defined and will be implemented.

- *Ensure that progress against EA plans is measured and reported.* To assist in attaining stated EA program goals and objectives, an organization should understand and disclose its progress against plans.

As EA products emerge, their content should be assessed against the plans to ensure that expectations are being met.

At Stage 4, during which organizations focus on architecture completion activities, organizations need to satisfy eight core elements:

- *Issue a written and approved organization policy for EA maintenance.* A policy promotes enterprisewide commitment to keeping the EA up to date. It should provide for establishing a process for architecture maintenance, including oversight and control. It should also identify the roles, responsibilities, and relationships of key players in the maintenance process.

- *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 a contractor that is not involved with any of the architecture development activities—verify and validate that the products were developed in accordance with architecture processes and product standards. Doing so provides organizations with needed assurance of the quality of the architecture.

- *Ensure that EA products describe both the "as is" and the "to be" environments, as well as a sequencing plan.* Consistent with the EA program plans discussed in Stage 2, an organization should ensure that the EA products completely and correctly describe both the "as is" and the "to be" environments of the enterprise and include a sequencing plan for migrating the organization between the two environments.

- *Ensure that EA products for both environments are described in terms of business, performance, information/data, application/service, and technology.* An organization's EA products should be defined and normalized in terms meaningful to a wide variety of stakeholders, ranging from the organization's chief executive officer and strategic planners to its technology implementers and operators.

- *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 architecture 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 the EA products.

- *Ensure that the organization's chief information officer has approved the current version of the EA.* The current version of the organization's completed EA should be approved by the CIO.

- *Ensure that a committee or group representing the enterprise or the investment review board has approved the current version of the EA.* The current version of the organization's completed architecture should also be approved either by the EA steering committee or by the investment review board.

- *Measure and report on the quality of EA products.* An organization should ensure that the nature and content of the EA products meet defined quality standards. This core element entails developing a set of metrics and assessing the products against those metrics.

At Stage 5, during which the focus is on architecture maintenance and implementation activities, organizations need to satisfy eight core elements:

- *Issue a written and approved organization policy for information technology (IT) investment compliance with the EA.* A policy that governs the implementation of the architecture should be approved by the organization head. The EA policy should augment architecture development and maintenance policies by providing for an institutional EA implementation process that is aligned with the organization's capital planning and investment control process.

- *Ensure that the organization has a process to formally manage EA change.* A formal process should be defined and implemented for introducing changes to the architecture. This process should recognize both internally and externally prompted change, and it should provide for continuous capture and analysis of change proposals and informed decision making about whether to make changes.

- *Make the EA an integral component of the IT investment management process.* Because the road map defines the IT systems that an organization plans to invest in as it transitions from the "as is" to the "to be" environment, the architecture is a critical frame of reference for making IT investment decisions. Using the architecture 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 road map.

- *Ensure that EA products are periodically updated.* An organization will need to periodically update its EA products depending on the volume and degree of approved changes to the EA.

- *Ensure that IT investments comply with EA.* An organization's IT investments should be aligned and comply with the applicable components of the current version of the EA, and they should not be selected and approved under the organization's capital planning and investment control process unless compliance is documented by the investment sponsor and substantiated by the architect assessment team.

- *Ensure that the organization head has approved the current version of the EA.* The current version of the EA should ultimately be approved by the head of the organization.

- *Measure and report return on EA investment.* Like any investment, the architecture 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 in order to ensure that expected benefits from the architecture are realized and to share this information with executive decision makers, who can then take corrective action to address deviations from expectations.

- *Measure and report on compliance with the EA.* An organization should define metrics, such as number of compliance waivers requested and number granted, to track compliance. Through such measurement and reporting, relevant trends and anomalies can be identified, and corrective action can be taken.

Assessment of the FBI's EA Efforts against GAO's EA Management Maturity Framework

Stage	Core element	Satisfied?	Comments
Stage 1: EA awareness	Agency is aware of EA.	Yes	The FBI has acknowledged the need for an EA, and the Director has made its development a management priority.
Stage 2: Building the EA management foundation	Adequate resources exist.	No	According to FBI officials, they have identified the financial and human capital resources needed to effectively manage the bureau's architecture program. While bureau officials stated they have adequate financial resources to fund the program, including sufficient contractor assistance, four of five core architect positions identified as being needed to staff the program office have not yet been filled.
	Committee or group representing the enterprise is responsible for directing, overseeing, or approving EA.	Yes	The FBI has established an Enterprise Architecture Board to direct, oversee, and approve the EA. The board includes upper-level management from all the operating units, including the counterterrorism, counterintelligence, and finance divisions. Technical representatives, such as the chief technology officer and chief architect, also serve on this board.
	Program office responsible for EA development and maintenance exists.	Yes	The FBI has established a program office, called the Enterprise Architecture Unit, which is located in the CIO's office. The program office is responsible for the development, implementation, and maintenance of the EA.
	Chief architect exists.	Yes	The FBI has designated a chief architect.
	EA is being developed using a framework, methodology, and automated tool.	No	The FBI initially used the Federal Enterprise Architecture Framework and has since switched to OMB's five Federal Enterprise Architecture Reference Models. The bureau is using the Popkin System Architect tool. However, the bureau does not have a documented methodology that defines how EA products are to be developed. Instead of a defined methodology, the bureau is relying on a combination of its chief architect's knowledge and certain documentation, such as an EA alignment plan that describes, among other things, the products to be developed, the order in which they are to be developed, the relationships among products, and analyses that are to be performed to help identify gaps and redundancies in the contents of these products. However, this documentation does not include either the specific steps or methods that explain how the content of products is to be developed and documented.

(Continued From Previous Page)

Stage	Core element	Satisfied?	Comments
	EA plans call for describing the "as is" and "to be" environments, and a sequencing plan.	Yes	The EA program management plan (dated October 2004) calls for the development of "as is" and "to be" environments as well as a sequencing plan.
	EA plans call for describing the enterprise in terms of business, performance, information/data, application/service, and technology.	Yes	The FBI's EA baseline report (dated March 2005) and other plans call for the development of business, performance, data, applications, and technology descriptions.
	EA plans call for business, performance, information/data, application/service, and technology descriptions to address security.	Yes	The FBI's EA baseline report (dated March 2005) and other plans call for security services to be defined for each of the descriptions.
	EA plans call for developing metrics for measuring EA progress, quality, compliance, and return on investment.	Yes	The EA policy (dated August 2003) and program management plan call for developing metrics to measure progress, quality, and return on investment.
Stage 3: Developing EA products[a]	Written and approved organization policy exists for EA development.	Yes	The FBI has a written policy for EA development (dated August 2003) that was approved and signed by the CIO.
	EA products are under configuration management.	Yes	The bureau has a configuration management plan that defines management structures and processes for identifying, tracking, monitoring, reporting, and auditing changes to the architecture products. EA products, such as the program management plan, EA principles, initial versions of the "as is" architecture, and EA software tool, have been identified and placed under configuration management in accordance with the plan.
	EA products describe or will describe the enterprise's business, performance, information/data, application/service, and the technology that supports them.	Yes	The FBI is in the process of developing its "as is" and "to be" architectures. It reports that to date, it has issued what it describes as "high level" versions of each, but that these versions need additional work to be complete. The initial version of the "to be" includes the enterprise's business, performance, information/data, service, and technology descriptions. The latest draft of the "as is" also includes all of these descriptions, except performance. According to FBI officials, performance was omitted due to an oversight on their part, and they intend to address performance in the next version of the "as is" architecture.
	EA products describe or will describe the "as is" and the "to be" environments, and a sequencing plan.	Yes	The FBI is in the process of developing its "as is" and "to be" architectures. It reports that to date, it has issued what it describes as "high level" versions of each, but that these versions need additional work to be complete. The FBI also reports that it has developed a "high level" description of a sequencing plan that is not yet complete.

(Continued From Previous Page)

Stage	Core element	Satisfied?	Comments
	Business, performance, information/data, application/service, and technology address or will address security.	Yes	The FBI is in the process of developing its "as is" and "to be" architectures, as described above. These versions of its architectures include a description of security services. According to FBI officials, these versions are not yet complete.
	Progress against EA plans is measured and reported.	Yes	The FBI is measuring and reporting progress against EA plans.
Stage 4: Completing EA products[a]	Written and approved organization policy exists for EA maintenance.	No	The FBI does not have a written and approved policy for EA maintenance. While the bureau has an EA development policy, it does not address architecture maintenance, nor does it assign responsibility and accountability for maintenance.
	EA products and management processes undergo independent verification and validation.	Yes	While EA products and processes to date have not been independently verified and validated, the FBI hired a contractor in April 2005 to begin performing such assessments on both the EA products and the processes used to develop them.
	EA products describe the enterprise's business, performance, information/data, application/service, and the technology that supports them.	No	Initial EA products describe the enterprise's business, performance, information/data, application/service, and the technology that supports them. However, the FBI reports that these products are not completed.
	EA products describe the "as is" and the "to be" environments, and a transitioning (sequencing) plan.	No	Initial EA products describe the "as is" and the "to be" environments and a sequencing plan. However, the FBI reports that these products are not completed.
	Business, performance, data, application, and technology descriptions address security.	No	Initial EA products include business, performance, information/data, application/service, and the technology descriptions that address security. However, the FBI reports that these products are not completed.
	Organization's chief information officer has approved current version of EA.	No	The FBI is in the process of completing its EA, and when completed, the CIO plans to approve it.
	Committee or group representing the enterprise or the investment review board has approved current version of EA.	No	The FBI is in the process of completing its EA, and when completed, the Enterprise Architecture Board plans to approve it.
	Quality of EA products is measured and reported.	No	Although the FBI is in the process of completing its EA products, it is not currently measuring and reporting quality. FBI plans call for the bureau to begin measuring and reporting EA product quality starting in fiscal year 2006.
Stage 5: Leveraging the EA for managing change[a]	Written and approved policy exists for IT investment compliance with EA.	No	The FBI does not have a written and approved policy addressing IT investment compliance with EA.

(Continued From Previous Page)

Stage	Core element	Satisfied?	Comments
	Process exists to formally manage EA change.	Yes	The FBI configuration management plan defines a process to formally manage EA change. To manage the process, the bureau established a change management board in January 2003. The board reviews and determines whether to approve changes to the current FBI environment.
	EA is integral component of IT investment management process.	No	The FBI is in the process of completing its EA, and thus, it is not yet an integral part of the bureau's IT investment process.
	EA products are periodically updated.	No	The FBI is in the process of completing its EA, and when it is complete, bureau plans call for the products to be periodically updated.
	IT investments comply with EA.	No	All IT investments are not evaluated for compliance with a completed EA.
	Organization head has approved current version of EA.	No	The FBI does not yet have a completed EA for the Director to approve.
	Return on EA investment is measured and reported.	No	The FBI is not yet measuring and reporting return on investment.
	Compliance with EA is measured and reported.	No	The FBI is not yet measuring and reporting EA compliance.

Source: GAO analysis of FBI data.

[a]To achieve a particular stage includes satisfying the specified elements in the stage plus all elements from previous stages. For example, to achieve Stage 3 requires achieving the Stage 3-specific elements plus those in Stages 1 and 2.

Comments from the Federal Bureau of Investigation

August 15, 2005

Mr. Randolph C. Hite
Director, Information Technology
Architecture and Systems Issues
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Hite:

      Re: FBI RESPONSE TO GAO'S DRAFT REPORT, "FBI IS
          TAKING STEPS TO DEVELOP AN ENTERPRISE
          ARCHITECTURE, BUT MUCH REMAINS TO BE
          ACCOMPLISHED," GAO-05-363

      Thank you for affording the FBI the opportunity to
review and provide comments on the GAO Draft Audit Report
entitled "FBI is Taking Steps to Develop an Enterprise
Architecture, But Much Remains to be Accomplished." We
appreciate the GAO's assessment and feedback on the FBI
Enterprise Architecture (EA) program development as well as its
recognition that we have made "important progress from the
bureau's status 2 years ago." The GAO's report provides
recommendations to ensure that effective contracting management
practices are employed in the development of the EA.
Furthermore, the GAO's report assesses the status of the FBI EA
program based on 32 core elements that include many federal EA
best practices as defined in GAO's Enterprise Architecture
Maturity Model Framework (EAMMF). The GAO EAMMF provides the
basis for assessing federal EA program maturity ranging from
Stage 1 through 5. Significant progress has been made at the FBI
since the formation of a new Enterprise Architecture Program in
the Office of the Chief Information Officer (OCIO) in January
2004. The FBI has reviewed the report and its recommendations
and will continue to strive towards the development of a robust
EA program supported by effective contracting management
practices.

      While the GAO report recommended performance-based
contracting as one of the preferred approaches, the FBI has been
successful with the fixed-price contracting methodology used for
its EA contractor support. Using a Firm Fixed Price (FFP)
contract for the EA contractor has been successful because the

Mr. Randolph C. Hite:

contractor has a financial incentive to stay on schedule and
provide deliverables listed in the statement of work. In a FFP
agreement, the contractor assumes the risk for any cost overrun
incurred. The FBI is following its *EA Program Management Plan
(PMP)* and the Federal CIO Council's *Practical Guide to Federal
Enterprise Architecture* to manage the contractor and the
program's development. Since the development of the EA is an
evolving practice, the use of a FFP contract increases the
likelihood that the FBI would award to a contractor who maintains
an awareness of evolving EA expectations and had complete
confidence in their ability to perform since the contractor
assumes most of the risk. The FBI uses a disciplined project
management approach with its EA contractor, requiring regular
project status reports and EA product reviews. All EA artifacts
are thoroughly monitored by the EA Program Office (EAPO) and are
submitted to a FBI Architecture Working Group for review,
validation, and quality assurance checks. These checks and
balances, which are standard processes for all EA products,
ensure that the FBI is receiving timely, complete, and accurate
deliverables from its EA contractor. Additionally, the FBI's EA
contractor indicated that it's ability to perform under the FBI
approach has been more successful than other government
approaches. The FBI recognizes GAO's recommendation for
performance-based contracting and is currently taking steps to
increase the use of performance-based contracting where
appropriate. The FBI Finance Division is using an independent
contractor to increase awareness and provide the appropriate
training for performance-based contracting.

        The GAO identified two remaining elements in the EAMMF
that are required for the FBI to be fully compliant with Stage 3,
the basic foundation for development of an EA. According to GAO,
the FBI has successfully completed 14 of the 16 total elements in
Stages 1-3 in the GAO EAMMF. The FBI is completing the following
for Stage 3 maturity: (1) thoroughly document the FBI's EA
development methodology and (2) provide adequate resources. The
FBI has drafted the documentation for the methodology that has
been successfully used in the EA program to develop key
architecture products like the As-Is Baseline and the To-Be
Target Architecture reports. It is currently pending final
management approval. Once approved, it will be provided to the
GAO. The FBI already has four senior level positions posted with
the Office of Personnel Management (OPM) with selection
forthcoming soon. We will provide an updated status to GAO in
order to satisfy the two remaining elements required in the EAMMF
for Stage 3 compliance. While the existing EA continues to
advance, it now provides a clear roadmap to help the FBI more
effectively develop systems that directly support its mission.

2

Mr. Randolph C. Hite:

      In the overall picture of EA design government-wide, the FBI has made significant progress with its EA development as it has approached Stage 3 compliance in 18 months. The FBI appreciates GAO's assessment that we have successfully satisfied one core element in Stage 4 and another in Stage 5. The GAO has recognized that the FBI is now in compliance with 16 of the EAMMF's 32 elements necessary for a mature EA. By continuing to make the EA Program a top priority within the OCIO, we expect to continue to mature the FBI EA into an actionable and enforceable architecture evidenced by an eventual Stage 4 and Stage 5 assessment. From that point, the FBI will continue to ensure the architecture properly reflects its evolving mission and business practices.

      Again, thank you for the opportunity to respond to the report. Should you or your staff have questions regarding our response, please feel free to contact me or any of my EA staff.

      Mr. Sanjeev Bhagowalia
      (Acting) Project Management Executive
      Office of IT Policy and Planning
      Sonny.Bhagowalia@ic.fbi.gov
      202-324-1210

      Mr. Shau-Fai Tse
      Unit Chief
      Enterprise Architecture Unit
      Shau-Fai.Tse@ic.fbi.gov
      202-324-6102

      Dr. M. Wayne Shiveley
      Chief Enterprise Architect
      Enterprise Architecture Unit
      Murle.Shiveley@ic.fbi.gov
      202-324-6750

                    Sincerely yours,

                    Zalmai Azmi
                    Chief Information Officer

3

GAO Contact and Staff Acknowledgments

GAO Contact

Randolph C. Hite, (202) 512-3439

Acknowledgments

In addition to the contact named above, the following people made key contributions to this report: Gary Mountjoy, Assistant Director; Barbara Collier; Lori Martinez; Teresa Neven; and William Wadsworth.

GAO's Mission	The Government Accountability 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 GAO's Web site (www.gao.gov). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "Subscribe to Updates."

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. Government Accountability 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
Congressional Relations	Gloria Jarmon, Managing Director, JarmonG@gao.gov (202) 512-4400 U.S. Government Accountability Office, 441 G Street NW, Room 7125 Washington, D.C. 20548
Public Affairs	Paul Anderson, Managing Director, AndersonP1@gao.gov (202) 512-4800 U.S. Government Accountability Office, 441 G Street NW, Room 7149 Washington, D.C. 20548